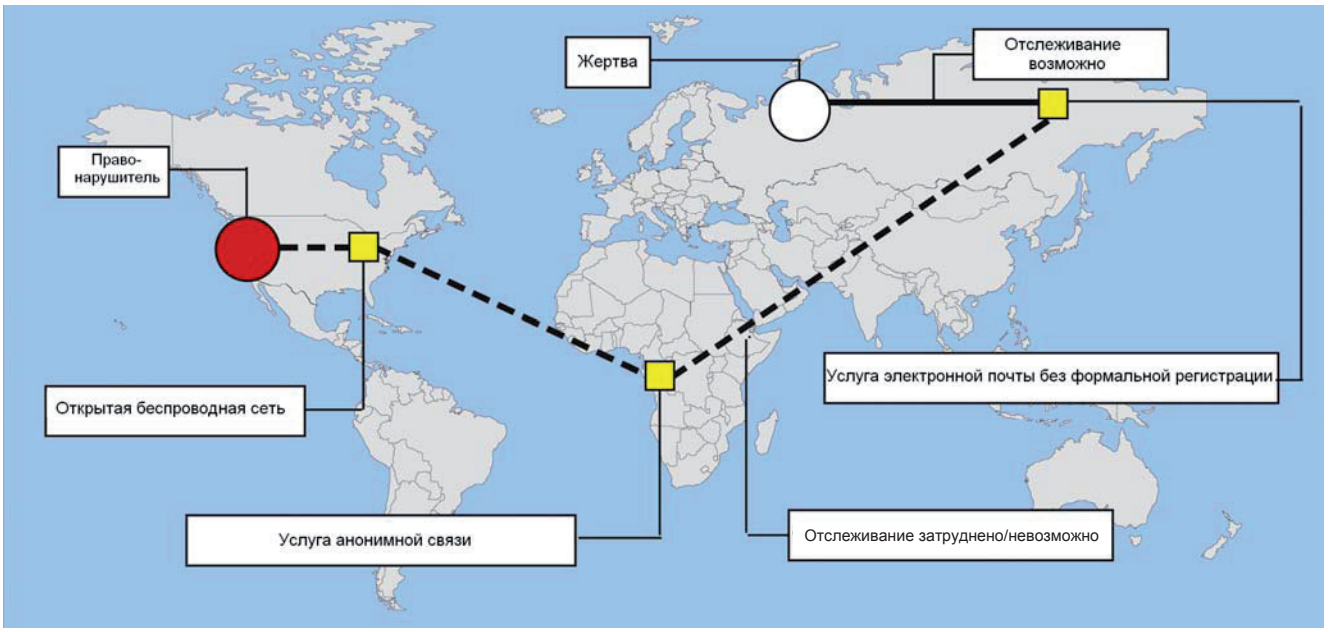
Международный союз электросвязи



Понимание киберпреступности: Руководство для развивающихся стран

Отдел приложений ИКТ и кибербезопасности
Департамент политики и стратегии
Сектор развития электросвязи МСЭ

Проект. Апрель 2009 г.

Для получения более подробной информации обращайтесь
в Отдел приложений ИКТ и кибербезопасности МСЭ-D по адресу: cybmail@itu.int

Международный союз электросвязи

Благодарности

Данный Отчет был подготовлен по заказу Отдела приложений ИКТ и кибербезопасности Сектора развития МСЭ.

Документ "Понимание киберпреступности: Руководство для развивающихся стран" был подготовлен др. Марко Герке. Автор хотел бы поблагодарить команду Сектора развития электросвязи МСЭ за поддержку и Гунхилда Шира за интенсивные дискуссии.

Используемые в настоящей публикации обозначения и классификации не отражают какого-либо мнения в отношении правового или иного статуса любой территории, либо одобрения или признания каких бы то ни было границ. Термин "страна" в настоящей публикации относится к странам и территориям.

Публикация МСЭ "Понимание киберпреступности: Руководство для развивающихся стран" доступно в онлайновом режиме по адресу:

www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

Этот документ отформатирован для двусторонней печати. Этот документ выпущен без официального форматирования.

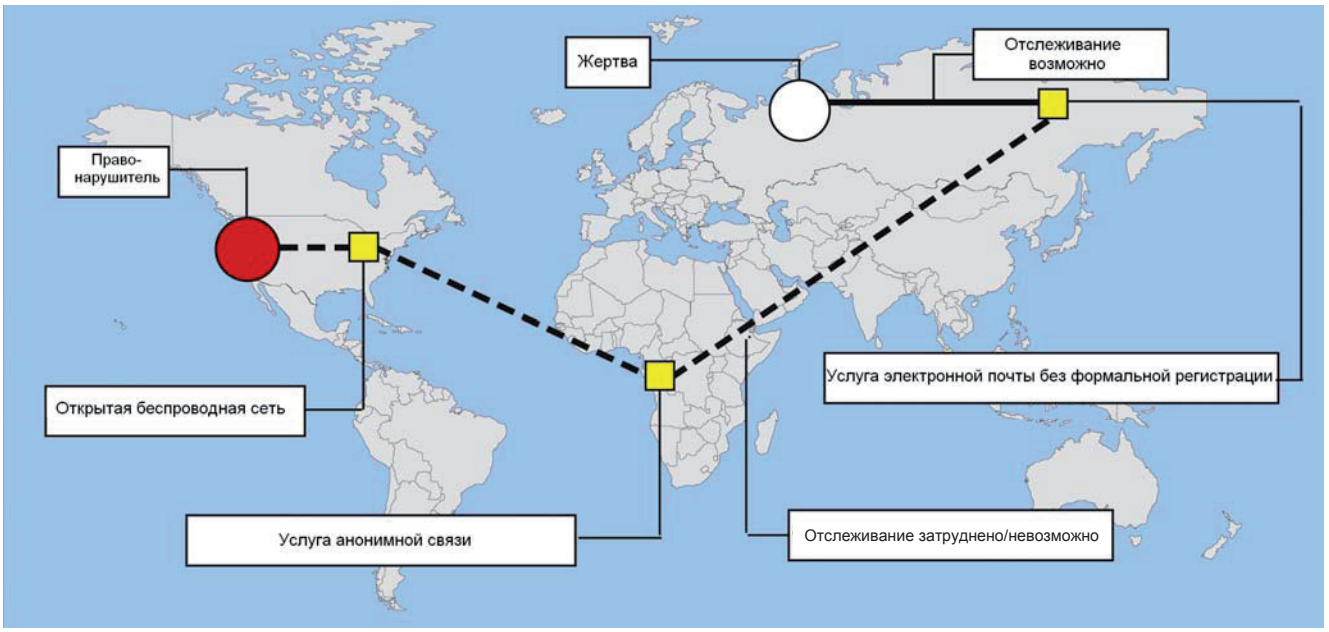
Для получения более подробной информации, пожалуйста, обращайтесь:

Отдел приложений ИКТ и кибербезопасности (CYB)
Департамент политики и стратегии
Бюро развития электросвязи
Международный союз электросвязи
Place des Nations
1211 Geneva 20
Switzerland
Тел.: +41 22 730 5825/6052
Факс: +41 22 730 5484
Эл. почта: cybmail@itu.int
Веб-сайт: www.itu.int/ITU-D/cyb/

Правовая оговорка

Мнения, выраженные в данном отчете, являются мнениями автора(ов) и не обязательно отражают точки зрения Международного союза электросвязи (МСЭ) или его членов. Использованные обозначения и представление материала, включая карты, не предполагают выражения какого-либо мнения со стороны МСЭ относительно правового статуса любой страны, территории, города или области, или относительно определения их границ или государственных границ. Указания и ссылки на конкретные страны, компании, продукты, инициативы или руководства ни в коем случае не предполагают, что МСЭ одобряет или рекомендует их как предпочтительные по сравнению с иными аналогичными компаниями, продуктами, инициативами и руководствами, которые не упоминаются.

Международный союз электросвязи



Понимание киберпреступности: Руководство для развивающихся стран

Отдел приложений ИКТ и кибербезопасности
Департамент политики и стратегии
Сектор развития электросвязи МСЭ

Проект. Апрель 2009 г.

Для получения более подробной информации обращайтесь
в Отдел приложений ИКТ и кибербезопасности МСЭ-D по адресу: cybmail@itu.int

Международный союз электросвязи

Сокращения

ABA	American Bar Association		Американская ассоциация адвокатов
APEC	Asia-Pacific Economic Cooperation Forum	АТЭС	Форум Азиатско-Тихоокеанского экономического сотрудничества
APIG	All Party Internet Group		Объединенная группа проблем интернета
ASEAN	Association of Southeast Asian Nations		Ассоциация государств Юго-Восточной Азии
CFAA	Computer Fraud and Abuse Act (U.S.)		Закон о компьютерном мошенничестве и злоупотреблениях (США)
CMA	Computer Misuse Act (U.K.) & Computer Misuse Act (Singapore)		Закон о неправомерном использовании компьютерных технологий (Соединенное Королевство) и Закон о неправомерном использовании компьютерных технологий (Сингапур)
CoE	Council of Europe		Совет Европы
DDoS	Distributed Denial of Service		Распределенный отказ в обслуживании
EC	European Commission		Европейская комиссия
EC Regulations	Privacy and Electronic Communications Regulations 2003 (United Kingdom)		Положение о частной информации и электронной связи 2003 г. (Соединенное Королевство)
ECPA	Electronic Communications Privacy Act (U.S.)		Закон о конфиденциальности электронных сообщений (США)
EU	European Union	ЕС	Европейский союз
G8	Group of Eight Nations		Группа восьми
GCA	Global Cybersecurity Agenda	ГПК	Глобальная программа кибербезопасности
IAG	International Assistance Group (Canada)		Международная группа поддержки (Канада)
ICT	Information and Communication Technology	ИКТ	Информационно-коммуникационные технологии
IRG	Gesetz über die Internationale Rechtshilfe in Strafsachen		
ITU	International Telecommunication Union	МСЭ	Международный союз электросвязи
OECD	Organization for Economic Cooperation and Development	ОЭСР	Организация экономического сотрудничества и развития
OWig	Gesetz über Ordnungswidrigkeiten (Germany)		
PACC	ABA Privacy & Computer Crime Committee		Комитет ABA по конфиденциальности и компьютерным преступлениям
RIPA	Regulation of Investigatory Powers Act (United Kingdom)		Закон о правовом регулировании следственных полномочий (Соединенное Королевство)
StGB	German Criminal Code (Strafgesetzbuch)		Уголовный кодекс Германии (Strafgesetzbuch)
StPO	German Code of Criminal Procedure (Strafprozessordnung)		Уголовно-процессуальный кодекс Германии (Strafprozessordnung)
TKG	German Telecommunications Act (Telekommunikationgesetz)		Закон об электросвязи Германии (Telekommunikationgesetz)
U.K.	United Kingdom		Соединенное Королевство
UN	United Nations	ООН	Организация Объединенных Наций
UrhG	German Copyright Act (Urheberrechtsgesecht)		Закон об авторском праве Германии (Urheberrechtsgesecht)
U.S.	United States	США	Соединенные Штаты Америки
WSIS	World Summit on the Information Society	ВВУИО	Всемирная встреча на высшем уровне по вопросам информационного общества

Цель

Целью документа **Понимание киберпреступности: Руководство для развивающихся стран** является содействие странам в понимании законодательных аспектов кибербезопасности и помощь в гармонизации законодательных основ. Таким образом, Руководство имеет своей целью помочь развивающимся странам лучше понять национальные и международные последствия возрастающих киберугроз, оценить потребности существующих национальных, региональных и международных инструментов, а также оказать содействие странам в создании устойчивых законодательных основ.

Данное Руководство содержит исчерпывающий обзор большинства необходимых тем, связанных с законодательными аспектами киберпреступности. При таком подходе данное Руководство сфокусировано на потребностях развивающихся стран. Из-за транснациональных масштабов киберпреступности, законодательные инструменты являются одинаковыми для развивающихся и для развитых стран. Однако справочные документы были отобраны, исходя из потребностей развивающихся стран. Данное Руководство содержит широкий выбор ресурсов для более глубокого изучения различных тем. Везде, где это возможно, использованы доступные опубликованные источники, включая множество бесплатных изданий или онлайновых юридических журналов.

Данное Руководство содержит шесть основных глав. После введения (*Глава 1*) Руководство содержит обзор явления киберпреступности (*Глава 2*). Он включает в себя описание того, как совершаются преступления и объяснения наиболее широкораспространенных противоправных действий в сфере киберпреступлений, таких как хакерство, кража идентичности и атаки типа "Отказ в обслуживании". Данное Руководство, кроме того, содержит обзор задач, связанных с расследованием и наказанием киберпреступности (*Главы 3* и *4*). После краткого описания некоторых из действий, предпринятых международными и региональными организациями в рамках борьбы с киберпреступностью (*Глава 5*), Руководство содержит анализ различных законодательных подходов, связанных с материальным уголовным правом, процессуальным правом, международным сотрудничеством и ответственностью поставщиков услуг интернета (*Глава 6*), включая примеры международных подходов, а также примеры рекомендуемых действий из национальных решений.

Документ **Понимание киберпреступности: Руководство для развивающихся стран** рассматривает первую из семи стратегических целей Глобальной программы кибербезопасности МСЭ (ГПК), которая призывает к тщательной разработке стратегий для создания законодательства по борьбе с киберпреступностью, которое было бы применимо на глобальном уровне и взаимодействовало бы с существующими национальными и региональными законодательными актами, а также рассматривает разрабатываемый Исследовательской комиссией МСЭ-D в рамках Вопроса 22/1 подход по организации национальных усилий по борьбе с киберпреступностью. Создание национальной правовой инфраструктуры является составной частью национальной стратегии кибербезопасности. Принятие всеми государствами соответствующего законодательства по борьбе со злоупотреблением информационными и коммуникационными технологиями в преступных или иных целях, включая действия, призванные воздействовать на целостность важнейших национальных информационных инфраструктур, является центральным пунктом для достижения глобальной кибербезопасности. Поскольку угрозы могут исходить из любой точки Земного шара, эта задача, в своей основе, является международной и требует международного сотрудничества, содействия в расследовании преступлений и общих оперативных и процессуальных положений. Следовательно, важно чтобы страны гармонизировали свои правовые основы для борьбы с киберпреступностью и упрощения международного сотрудничества.

Содержание

1 ВВЕДЕНИЕ

1.1 Инфраструктура и услуги

Интернет – это одна из наиболее быстро растущих областей развития технической инфраструктуры[1]. Сегодня информационно-коммуникационные технологии (ИКТ) представлены повсюду и тенденции их цифровизации постоянно растут. Спрос на интернет и компьютерные соединения привел к интеграции компьютерных технологий в продукты, которые обычно работали без них, например автомобили и здания[2]. Электропитание, транспортная инфраструктура, военная служба и логистика – практически все современные услуги зависят от использования ИКТ[3].

Хотя развитие новых технологий сфокусировано, главным образом, на удовлетворении потребительского спроса в западных странах, развивающиеся страны также могут пользоваться преимуществами новых технологий[4]. При доступности технологий дальней беспроводной связи, например WiMAX[5] и компьютерных систем, которые сегодня имеют цену менее 200 долл. США[6], гораздо больше людей в развивающихся странах должны иметь более простой доступ в интернет и связанным с ним продуктам и услугам[7].

Влияние ИКТ на общество простирается намного дальше, чем создание базовой информационной инфраструктуры. Готовность ИКТ является основой для разработки критериев создания, готовности и использования сетевых услуг[8]. Электронная почта заменила традиционные письма[9]; онлайновые веб-презентации сегодня имеют более важное значение для бизнеса, чем печатные рекламные материалы[10]; и услуги связи и телефонии на базе интернета растут быстрее, чем проводная связь[11].

---

1 Related to the development of the Internet, see: *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th international conference on Electronic commerce, Page 52 – 56; The World Information Society Report 2007, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/. According to the ITU, there were 1,13 billion Internet users by the end of 2007, available at: http://www.itu.int/ITU-D/.

2 Regarding the threat of attacks against computer systems integrated in cars, see: BBC News, Cars safe from computer viruses, 11.05.2005, available at: http://news.bbc.co.uk/1/hi/technology/4536307.stm.

3 See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1. *Bohn/Coroama/Langheinrich/Mattern/Rohs,* "Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications", Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 et seqq., available at: http://www.vs.inf.ethz.ch/res/papers/hera.pdf. A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm, 'sasser". In 2004, the computer worm affected computers running versions of Microsoft's operation System Windows. As a result of the worm, a number of services were interrupted. Among them were the U.S. airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: http://www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

4 Regarding the possibilities and technology available to access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: http://www2007.org/workshops/paper_106.pdf.

5 WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services (such as access to the Internet) over long distances. For more information, see: The WiMAX Forum, available at http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, Fundamentals of WiMAX: Understanding Broadband Wireless Networking; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

6 Within the "One Laptop per Child" initiative, inexpensive laptop computers should be distributed to children, especially those in developing countries. The project is organised by the United States-based non-profit organisation OLPC. For more information, see the official OLPC website at http://www.laptop.org. Regarding the technology of the laptop, see Heise News, Test of the 100 dollar laptop, 09.05.2007, available at: http://www.heise.de/english/newsticker/news/89512.

7 Current reports highlight that less than 4 per cent of the African population has access to the Internet. See Waters, Africa waiting for net revolution, BBC News, 29.10.2007, available at: http://news.bbc.co.uk/1/hi/technology/7063682.stm.

8 Regarding the impact of ICT on the society see the report Sharpening Europe's Future Through ICT – Report from the information society technologies advisory group, 2006, available at: ftp://ftp.cordis.europa.eu/pub/ist/docs/istag-shaping-europe-future-ict-march-2006-en.pdf.

9 Regarding the related risks of attacks against e-mail systems see the report that United States Department of Defence had to shut down their e-mail system after a hacking attack. See: http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

10 Regarding the ability to block Internet-based information services by denial-of-service attacks see below 2.4.e.

11 Regarding the related difficulties of lawful interception of Voice over IP communication see *Bellovin and others*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at: http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, "Voice over IP: Forensic Computing Implications",

Доступность ИКТ и новые сетевые услуги предлагают множество преимуществ для общества в целом, особенно, для развивающихся стран.

Приложения ИКТ, такие как электронное правительство, электронная коммерция, электронное образование, электронное здравоохранение и электронная охрана окружающей среды, считаются движущими силами развития, поскольку они обеспечивают эффективный канал для предоставления широкого спектра базовых услуг в удаленных и сельских областях. Приложения ИКТ могут упростить в развивающихся странах достижение целей развития тысячелетия по здравоохранению и охране окружающей среды. Учитывая правильные подходы, контекст и процессы внедрения, инвестиции в приложения и инструменты, ИКТ могут привести к повышению производительности и улучшению качества. В свою очередь, приложения ИКТ могут освободить технические и людские ресурсы и обеспечить более обширный доступ к базовым услугам. В этом свете онлайновая кража идентичности и действия по получению в интернете удостоверяющей и/или личной информации другого человека для мошеннического ее использования в преступных целях сегодня является одной из основных угроз для дальнейшего развития услуг электронного правительства и электронного бизнеса[12].

Стоимость услуг часто также намного ниже, чем для сравниваемых услуг за пределами сети[13]. Услуги электронной почты часто бесплатны или стоят очень немного по сравнению с традиционными почтовыми услугами[14]. Онлайновая энциклопедия Wikipedia[15] может использоваться бесплатно, как и сотни онлайновых услуг хостинга[16]. Более низкие цены важны, так как они позволяют предоставлять услуги большему числу пользователей, включая людей с очень ограниченными доходами. Учитывая ограниченные финансовые ресурсы множества людей в развивающихся странах, интернет позволяет им использовать услуги, к которым они не могли бы получить доступа вне сети.

1.2 Преимущества и риски

Введение ИКТ во многие аспекты ежедневной жизни привело к разработке современной концепции Информационного общества[17]. Такое развитие Информационного общества обеспечивает широкие возможности[18]. Неограниченный доступ к информации может поддерживать демократию, так как поток информации выходит из-под контроля государственных чиновников (как это произошло, например в Западной Европе)[19]. Технические достижения улучшили ежедневную жизнь, например, онлайновые банковские операции и совершение онлайновых покупок, использование услуг подвижной передачи данных

2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

12 *ITU*, ICT Applications and Cybersecurity Background Note to the 2009 Pacific ICT Ministerial Forum held in Tonga 17-20 February 2009, 2009, available at: http://www.itu.int/ITU-D/asp/CMS/Events/2009/PacMinForum/doc/Background%20Note-Theme-4-ICT%20Apps%20&%20Cybersecurity.pdf.

13 Regarding the possibilities of low cost access the Internet in developing countries, see: *Esteve/Machin*, Devices to access Internet in Developing countries, available at: http://www2007.org/workshops/paper_106.pdf.

14 Regarding the number of users of free-or-charge e-mail services see *Graham*, Email carriers deliver gifts of ninety features to lure, keep users, USA Today, 16.04.2008, available at: http://www.usatoday.com/tech/products/2008-04-15-google-gmail-webmail_N.htm. The article mentions that the four biggest webmail providers have several hundred million users – Microsoft (256 million), Yahoo (254 million), Google (91 million) and AOL (48 million). For an overview on e-mail statistics see: *Brownlow*, e-mail and web statistics, April 2008, available at: http://www.email-marketing-reports.com/metrics/email-statistics.htm.

15 http://www.wikipedia.org

16 Regarding the use of free-of-charge services in criminal activities See for example: Symantec Press Release, Symantec Reports Malicious Web Attacks Are on the Rise, 13.05.2008, available at: http://www.symantec.com/business/resources/articles/article.jsp?aid=20080513_symantec_reports_malicious_web_attacks_are_on_the_rise.

17 Unlike in the Industrial Society, members of the Information Society are no longer connected by their participation in industrialisation, but through their access to and the use of ICTs. For more information on the information society see: *Masuda*, The Information Society as Post-Industrial Society; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe; *Maldoom/Marsden/Sidak/Singer*, Broadband in Europe: How Brussels can wire the Information Society; Salzburg Center for International Legal Studies, Legal Issues in the Global Information Society; *Hornby/Clarke*, Challenge and Change in the Information Society.

18 See for example: Communication From The Commission To The Council, The European Parliament, The European Economic And Social Committee And The Committee Of The Regions, Challenges for the European Information Society beyond 2005, page 3, available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/communications/new_chall_en_adopted.pdf.

19 Regarding the impact of ICT on the development of the society see: *Barney*, Prometheus Wired;: The Hope for Democracy in the Age of Network Technology, 2001; *Yang*, Between Democracy and Development: The impact of new information technologies on civil societies in China, available at: http://programs.ssrc.org/itic/publications/civsocandgov/yangpolicyrevised.pdf; *White*, Citizen Electronic: Marx and Gilder on Information Technology and Democracy, Journal of Information Technology impact, 1999, Vol. 1, page 20, available at: http://www.jiti.com/v1n1/white.pdf.

и телефонии по протоколу Интернет (VoIP) – только некоторые приметы того, насколько глубоко проникли ИКТ в нашу повседневную жизнь[20].

Однако рост информационного общества сопровождается новыми и серьезными угрозами[21]. Жизненно важные службы такие как водо- и электроснабжение сегодня опираются на ИКТ[22]. Автомобили, регулировка движения, лифты, кондиционирование воздуха и телефоны также зависят от бесперебойной работы ИКТ[23]. Атаки на информационную инфраструктуру и услуги интернета сегодня способны причинить вред обществу новыми и критическими способами[24].

Атаки на информационную инфраструктуру и услуги интернета уже совершаются[25]. Онлайновое мошенничество, распространение детской порнографии и хакерские атаки – только некоторые примеры компьютерных преступлений, которые совершаются ежедневно в огромных масштабах[26]. Финансовый урон, наносимый киберпреступностью, чрезвычайно велик[27]. Только в 2003 году вредоносное программное обеспечение причинило ущерб на сумму до 17 миллиардов долл. США[28]. По некоторым оценкам, доходы от киберпреступности в 2007 году превысили 100 миллиардов долл. США, впервые превзойдя незаконную торговлю наркотиками[29]. Почти 60% предприятий в Соединенных Штатах Америки считают, что киберпреступность им обходится дороже, чем физическая преступность[30]. Эти оценки явно демонстрируют важность защиты информационных инфраструктур[31].

---

[20] Regarding the extend of integration of ICTs into the daily lives and the related threats see below 3.2.a as well as *Goodman*, "The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

[21] See *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, Page 212; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[22] See *Suter*, A Generic National Framework For Critical Information Infrastructure Protection, 2007, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf.

[23] *Bohn/Coroama/Langheinrich/Mattern/Rohs,* "Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications", Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 et seqq., available at: http://www.vs.inf.ethz.ch/res/papers/hera.pdf.

[24] See *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1, page 1; *Wilshuse*n, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: http://www.gao.gov/new.items/d08212t.pdf.

[25] Regarding the attack against online service in Estonia, see: *Toth*, Estonia under cyberattack, available at: http://www.cert.hu/dmdocuments/Estonia_attack2.pdf. Regarding the attacks against major online companies in the United States in 2000 see: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension", in Sofaer/Goodman, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", page 4, available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.

[26] The Online-Community HackerWatch publishes reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in one month (August 2007). Source: http://www.hackerwatch.org.

[27] See *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

[28] CRS Report for Congress on the Economic Impact of Cyber-Attacks, April 2004, Page 10, available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

[29] See: *O"Connell*, Cyber-Crime hits $ 100 Billion in 2007, ITU News related to ITU Corporate Strategy, 17.10.2007, available at: http://www.ibls.com/internet_law_news_portal_view_prn.aspx?s=latestnews&id=1882.

[30] IBM survey, published 14.05.2006, available at: http://www-03.ibm.com/industries/consumerproducts/doc/content/news/pressrelease/1540939123.html.

[31] *Wilshuse*n, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: http://www.gao.gov/new.items/d08212t.pdf.For more information on the economic impact of Cybercrime see below 2.9.

1.3 Кибербезопасность и киберпреступность

Кибербезопасность[32] играет важную роль в текущем развитии информационных технологий, а также интернет-услуг[33]. Усиление кибербезопасности и защита важнейших информационных инфраструктур имеет огромное значение для безопасности экономического благосостояния каждой страны. Повышение безопасности интернета и защита пользователей интернета стало составной частью разработки новых услуг, а также правительственной политики[34]. Сдерживание киберпреступности является составной частью национальной кибербезопасности и стратегии защиты важнейшей информационной инфраструктуры. В частности, это включает в себя принятие соответствующего законодательства против злонамеренного использования ИКТ в преступных или иных целях и для действий, целью которых является воздействие на целостность важнейших национальных инфраструктур. На национальном уровне это общая ответственность, требующая скоординированных действий со стороны правительственных организаций, частного сектора и граждан в отношении предупреждения, подготовки, реагирования и восстановления после инцидентов. На региональном и международном уровне это влечет за собой кооперацию и координацию с соответствующим партнерами. Таким образом, формулировка и внедрение национальных основ и стратегии кибербезопасности требует всеобъемлющего подхода[35]. Стратегии кибербезопасности, например, разработка технических защитных систем или обучение пользователей тому, как не стать жертвами киберпреступности, может содействовать снижению рисков киберпреступности[36]. Разработка и поддержка стратегий кибербезопасности является жизненно важным элементом в борьбе против киберпреступности[37].

Юридические, технические и организационные задачи, поставленные проблемой кибербезопасности, являются глобальными и далекоидущими и могут быть разрешены только посредством последовательной стратегии, учитывающей роль различных участников и существующие инициативы в рамках международного сотрудничества[38]. В этом отношении Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО)[39] признала реальные и значительные риски, обусловленные несоответствием кибербезопасности и быстрым распространением киберпреступности. Параграфы 108–110

---

[32] The term “Cybersecurity” is used to summarise various activities such as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. Regarding the definition of cybersecurity, ITU-T Recommendation X.1205 “Overview of Cybersecurity” provides a definition, description of technologies, and network protection principles. “Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality.” Also see *ITU*, List of Security-Related Terms and Definitions, available at: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc..

[33] With regard to development related to developing countries see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[34] See for example: ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006) available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; European Union Communication: Towards a General Policy on the Fight Against Cyber Crime, 2007, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[35] For more information, references and links see the ITU Cybersecurity Work Programme to Assist Developing Countries (2007-2009), 2007, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[36] For more information see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

[37] See: *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, available at: http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybercrime.pdf; See as well Pillar One ITU Cybersecurity Work Programme, available at: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html; With regard to the elements of an anti-cybercrime strategy see below: Chapter 4.

[38] See in this context: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[39] For more information on the World Summit on the Information Society (WSIS), see: http://www.itu.int/wsis/

Тунисской программы для информационного общества, принятой ВВУИО[40], включая Дополнение, устанавливают план для многосторонней реализации на международном уровне *Женевского плана действий ВВУИО*[41], описывающего процесс многосторонней реализации в соответствии с одиннадцатью направлениями деятельности и распределение ответственности за содействие реализации различных направлений деятельности. На ВВУИО мировые лидеры и правительства поручили МСЭ содействовать реализации Направления деятельности С5 ВВУИО, ориентированного на формирование атмосферы доверия и безопасности при использовании ИКТ[42].

В этой связи Генеральный секретарь МСЭ 17 мая 2007 года объявил Глобальную программу кибербезопасности (ГПК)[43], совместно с правительствами, промышленностью, региональными и международными организациями, академическими и исследовательскими институтами. ГПК – это глобальная основа для диалога и международного сотрудничества по координации международной реакции на растущие проблемы кибербезопасности и повышения доверия и безопасности в информационном обществе. Она строится на существующей работе, инициативах и партнерстве по разработке глобальных стратегий по решению сегодняшних задач, связанных с формированием атмосферы доверия и безопасности в использовании ИКТ. В самом МСЭ Глобальная программа кибербезопасности дополняет существующие программы работ МСЭ путем содействия осуществлению тремя секторами МСЭ деятельности в области кибербезопасности в рамках международного сотрудничества.

В ГПК поставлено семь основных стратегических целей, лежащих в пяти областях действия: 1) Правовые меры; 2) Технические и процедурные меры; 3) Организационные структуры; 4) Программа создания потенциала и 5) Международное сотрудничество[44].

Борьба с киберпреступностью требует всестороннего подхода. Учитывая, что одни технические меры не могут предотвратить преступлений, важно чтобы органы правопорядка имели право эффективно расследовать и наказывать киберпреступления[45]. Среди областей действия ГПК область "Правовые меры" сфокусирована на том, как разрешить законодательные проблемы, обусловленные преступными действиями, совершаемыми в сетях ИКТ на уровне, сравнимом с международным. Область "Технические и процедурные меры" сфокусирована на ключевых мерах продвижения принятия расширенных подходов к улучшению безопасности и управлению рисками в киберпространстве, включая схемы, протоколы и стандарты аккредитации. Область "Организационные структуры" сфокусирована на предотвращении кибератак, их обнаружении, реагировании на них, а также на кризисном управлении во время кибератак, включая защиту важнейших систем информационной инфраструктуры. "Программа создания потенциала" сфокусирована на разработке стратегических механизмов создания потенциала для повышения осведомленности, передачи "know-how" и увеличения кибербезопасности по планам национальной политики. И наконец, "Международное сотрудничество" сфокусировано на международном сотрудничестве, диалоге и координации в противодействии кибератакам.

Разработка адекватного законодательства и разработка в рамках этого подхода законодательных основ, связанных с киберпреступностью, является важнейшей частью стратегии кибербезопасности. Это требует, в первую очередь, чтобы положения материального уголовного права объявили незаконными такие действия, как компьютерное мошенничество, незаконный доступ, искажение информации, нарушение авторских прав и детская порнография[46]. Тот факт, что в уголовном кодексе существуют положения, применимые к аналогичным действиям, совершаемым вне сети, не означает, что они могут применяться также и к действиям, совершаемым по интернету[47]. Следовательно, для определения любых возможных пробелов жизненно важен тщательный анализ существующих национальных законов[48]. Помимо положений

---

[40] The WSIS Tunis Agenda for the Information Society, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0

[41] The WSIS Geneva Plan of Action, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0

[42] For more information on WSIS action line C5: Building confidence and security in the use of ICTs see: http://www.itu.int/wsis/c5/

[43] For more information on the Global Cybersecurity Agenda (GCA) see: http://www.itu.int/cybersecurity/gca/

[44] For more information see: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[45] For an overview about the most important instruments in the fight against Cybercrime see below: Chapter 6.2.

[46] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview about the most important substantive criminal law provisions see below: Chapter 6.1.

[47] See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 et. Seqq.

[48] For an overview of the cybercrime-related legislation and their compliance with the international standards defined by the Convention on Cybercrime see the country profiles provided on the Council of Europe website. Available at: http://www.coe.int/cybercrime/. [48] See for example the following surveys on national Cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.* , available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf;

материального уголовного права[49], органам правопорядка требуются необходимые инструменты для расследования киберпреступлений[50]. Такие расследования сами по себе представляют множество проблем[51]. Нарушители могут действовать практически из любого местоположения в мире и принимать меры для маскировки своей идентичности[52]. Приспособления и инструменты, требуемые для расследования киберпреступлений, могут достаточно сильно отличаться от тех, что используются для расследований обычных преступлений[53].

1.4 Международные масштабы киберпреступности

Киберпреступность часто имеет международные масштабы[54]. Электронные письма с незаконным содержанием часто проходят через множество стран во время передачи от отправителя до получателя, либо незаконное содержание хранится за пределами страны[55]. В рамках расследования киберпреступлений очень важно тесное сотрудничество между вовлеченными странами[56]. Существующие соглашения о юридической взаимопомощи основаны на формальных, сложных процедурах, которые часто отнимают много времени[57]. Следовательно, важно наладить процедуры быстрого реагирования на инциденты, а также на запросы международного сотрудничества[58].

Многие страны основывают свой режим двусторонней юридической взаимопомощи на принципе "обоюдное признание деяния преступлением"[59]. Расследования на глобальном уровне обычно ограничиваются теми преступлениями, которые являются преступлениями во всех участвующих странах. Несмотря на то, что существует множество правонарушений, которые могут преследоваться судебным порядком в любой части мира, важную роль играют региональные различия[60]. Одним из примеров является запрещенное содержание.

Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework - unauthorized access to computer systems - penal legislation in 44 countries, available at: http://www.mosstingrett.no/info/legal.html.

49 See below: Chapter 6.1.

50 See below: Chapter 6.1.

51 For an overview about the most relevant challenges in the fight against Cybercrime see below: Chapter 3.2.

52 One possibility to mask the identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, 'solutions for Anonymous Communication on the Internet", 1999; Regarding the technical discussion about traceability and anonymity, see: "CERT Research 2006 Annual Report", page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf; Regarding anonymous file-sharing systems see: *Clarke/Sandberg/Wiley/Hong*, "Freenet: a distributed anonymous information storage and retrieval system", 2001; *Chothia/Chatzikokolakis*, "A Survey of Anonymous Peer-to-Peer File-Sharing", available at: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Design", 2005.

53 Regarding legal responses to the challenges of anonymous communication see below: Chapter 6.2.11

54 Regarding the transnational dimension of cybercrime see: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

55 Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplyfing Data Storage and Management, 2005.

56 Regarding the need for international cooperation in the fight against Cybercrime, see: Putnam/Elliott, "International Responses to Cyber Crime", in *Sofaer/Goodman*, " Transnational Dimension of Cyber Crime and Terrorism", 2001, page 35 et seqq., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 1 et seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf

57 See below: Chapter 6.3.

58 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141.

59 Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf; *Plachta*, International Cooperation in the Draft United Nations Convention against Transnational Crimes, UNAFEI Resource Material Series No. 57, 114th International Training Course, page 87 et. seqq., available at: http://www.unafei.or.jp/english/pdf/PDF_rms/no57/57-08.pdf.

60 See below: Chapter 5.5. See for example the following surveys on national Cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide, 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework - unauthorized access to computer systems - penal legislation in 44 countries, available at: http://www.mosstingrett.no/info/legal.html.

Судебное преследование запрещенного содержания в различных странах различно[61]. Материалы, которые могут законно распространяться в одной стране, в другой стране вполне могут оказаться запрещенными[62].

Используемые в настоящее время компьютерные технологии во всем мире практически одинаковы[63]. За исключением проблем с языком и блоков питания, различия между компьютерными системами и сотовыми телефонами, продаваемыми в Азии и Европе, очень малы. Аналогичная ситуация складывается и вокруг интернета. Благодаря стандартизации, протоколы, используемые в странах Африканского континента, такие же, как и те, что используются в Соединенных Штатах Америки[64]. Стандартизация позволяет пользователям во всем мире получать доступ через интернет к одним и тем же услугам[65].

Вопрос заключается в том, какое влияние гармонизация глобальных технических стандартов оказывает на разработку национальных уголовных законов. В том, что касается запрещенного содержания, пользователи интернета могут получать доступ к информации из любой точки земного шара. Это позволяет им получать доступ к информации, которая законно доступна за рубежом, но может быть запрещенной в их собственной стране.

Теоретически, разработки, обусловленные технической стандартизацией, простираются далеко за пределы глобализации технологий и услуг и могут привести к гармонизации национальных законов. Однако, как показали переговоры по вопросам Первого протокола Конвенция о киберпреступности Совета Европы[66], принципы национального законодательства меняются намного медленнее технического развития[67].

Несмотря на то, что интернет может не признавать пограничного контроля, существуют средства для ограничения доступа к определенной информации[68]. Поставщик услуг доступа обычно может заблокировать определенные веб-сайты, а поставщик услуг, у которого размещен веб-сайт, может предотвратить доступ к информации для тех пользователей, которые, в соответствии с их IP-адресами, связаны с определенной страной ("IP-фильтрация")[69]. Обе меры могут быть обойдены, но тем не менее, они являются инструментами, которые могут использоваться для сохранения территориальных различий в глобальной сети[70]. Инициатива OpenNet[71] сообщает, что такой вид цензуры применяется примерно в двадцати странах[72].

1.5 Последствия для развивающихся стран

Отыскание стратегий и решений по противостоянию угрозам киберпреступности является основной задачей, особенно, для развивающихся стран. Полномасштабная стратегия борьбы с киберпреступностью обычно

---

61 The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Convention on Cybercrime, but addressed in an additional protocol. See below: Chapter 2.5.

62 With regard to the different national approaches towards the criminalisation of child pornography, See for example *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999.

63 Regarding the network protocols see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

64 The most important communication protocols are TCP (Transmission Control Protocol) and the IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

65 Regarding the technical standardisation see: OECD, Internet Address Space, Economic Consideration in the Management of IPv4 and in the Development of IPv6, 2007, DSTI/ICCP(2007)20/FINAL, available at: http://www.itu.int/dms_pub/itu-t/oth/06/15/T061500000A0015PDFE.pdf; Regarding the importance of single technical as well as single legal standards see: *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 et. seqq.

66 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189), available at http://www.conventions.coe.int.

67 Since parties participating in the negotiation could not agree on a common position on the criminalisation of the dissemination of xenophobic material, provisions related to this topic were integrated into a First Protocol to the Council of Europe Convention on Cybercrime.

68 See *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

69 This was for example discussed within the famous Yahoo-decision. See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: http://www.juriscom.net/en/uni/doc/yahoo/poullet.htm; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

70 A possibility to circumvent geo-targeting strategies is the use of proxy servers that are located abroad.

71 The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information see: http://www.opennet.net.

72 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

содержит меры технической защиты, но также юридические инструменты[73]. Разработка и реализация этих инструментов требует времени. Меры технической защиты являются особенно дорогостоящими[74]. Развивающиеся страны должны с самого начала интегрировать меры защиты в процесс развертывания интернета. Несмотря на то, что это может первоначально повысить стоимость услуг интернета, долгосрочный выигрыш от предотвращения затрат и повреждений, обусловленных киберпреступностью, во много раз превосходит любые первоначальные затраты на меры технической защиты и защиту сети[75].

Риски, связанные со слабыми мерами защиты, могут, в действительности, более сильно повлиять на развивающиеся страны из-за того, что у них меньше безопасность и защита[76]. Возможность защитить пользователей, а также компании, является фундаментальным требованием не только для обычных предприятий, но также и для интернет-компаний и предприятий с онлайновым бизнесом. В отсутствие интернет-безопасности развивающиеся страны могут столкнуться с большими трудностями в продвижении электронного бизнеса и участии в предоставлении онлайновых услуг.

Разработка технических мер по повышению кибербезопасности и соответствующего законодательства против киберпреступности очень важна как для развитых, так и для развивающихся стран. По сравнению со стоимостью введения мер обеспечения безопасности и защитных мер в компьютерные сети на более позднем этапе, вероятно, первоначальные меры, принятые непосредственно с самого начала, могут быть менее дорогостоящими. Развивающиеся страны должны с самого начала разрабатывать свои стратегии борьбы с киберпреступностью в соответствии с международными стандартами[77].

---

[73] See below: Chapter 4.

[74] See with regard to the costs of technical protection measures required to fight against spam: *OECD*, 'spam Issues in Developing Countries", DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at http://www.oecd.org/dataoecd/5/47/34935342.pdf.

[75] Regarding cybersecurity in developing countries see: World Information Society Report 2007, page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

[76] One example is spam. The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: "ITU Survey on Anti-Spam Legislation Worldwide 2005", page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. Due to their limited resources, spam may pose a more serious issue for developing countries than for industrialised countries. See OECD: 'spam Issue in Developing Countries", DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

[77] For more details about the elements of an anti-cybercrime strategy see below: Chapter 4.

2 ЯВЛЕНИЕ КИБЕРПРЕСТУПНОСТИ

2.1 Определения киберпреступности

Большая часть отчетов, рекомендаций и публикаций по вопросам киберпреступности начинаются с определения термина "киберпреступность"[78]. Одно общепринятое определение описывает киберпреступность как любое деяние, в котором инструментом, целью или местом преступных действий являются компьютеры или сети[79]. Одним из примеров международного подхода является Статья 1.1 Проекта Международной Конвенции по улучшению защиты от киберпреступности и терроризма (CISAC)[80], которая отмечает, что киберпреступностью называются действия в отношении кибернетических систем[81].
В некоторых определениях предприняты попытки учесть цели или намерения и более точно определить киберпреступность[82], определяя киберпреступность как "действия посредством компьютеров, которые либо *являются незаконными*, либо *считаются противоправными* некоторыми сторонами и которые могут быть совершены *при помощи глобальных электронных сетей*"[83].

Эти более точные описания исключают те случаи, когда физическое оборудование используется для совершения обычных преступлений, но они рискуют исключить преступления, которые считаются киберпреступлениями в международных соглашениях, например в "Конвенции о киберпреступности"[84]. Например человек, который создает USB[85]-устройства, содержащие злонамеренные программы, которые разрушают информацию в компьютере, если устройство к нему присоединено, совершает преступление,

---

[78] Regarding approaches to define and categorise cybercrime See for example: Cybercrime, Definition and General Information, Australian Institute for Criminology, available at: http://www.aic.gov.au/topics/cybercrime/definitions.html; Explanatory Report to the Convention on Cybercrime, No. 8. *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: http://www.crime-research.org/articles/cybercrime-in-france-overview/; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: http://www.fas.org/sgp/crs/terror/RL32114.pdf; Cybercrime, Report of the Parliamentary Joint Committee on the Australian Crime Commission, 2004, page 5, available at: http://www.aph.gov.au/Senate/Committee/acc_ctte/completed_inquiries/2002-04/cybercrime/report/report.pdf; *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.; *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37 *Forst,* Cybercrime: Appellate Court Interpretations, 1999, page 1;

[79] See for example: *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: http://www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 et. seqq.; *Goodman*, Why the Policy don"t care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469.

[80] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[81] *Art*icle 1
Definitions and Use of Terms
For the purposes of this Convention:
1. “cyber crime” means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention;
[...]

[82] See *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3.

[83] *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at: http://www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37

[84] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention see below: Chapter 6.1.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq*.; *Gercke*, National, Regional and International Aproaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seqq; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol 95, No.4, 2001, page 889 *et seq*.

[85] Universal Serial Bus (USB)

которое определяется Статьей 4 Конвенции о киберпреступности Совета Европы[86]. Однако действие по удалению данных с использованием физического устройства для копирования злонамеренного кода не совершается по глобальным электронным сетям и не может быть квалифицировано как киберпреступление в соответствии с вышеприведенным узким определением. Это действие было бы квалифицировано как киберпреступление только в соответствии с определением, основанным на более широком описании, включающем такие действия как незаконное искажение информации.

Это показывает, что определение термина "киберпреступность" встречает заметные трудности[87]. Термин "киберпреступность" используется для описания широкого спектра правонарушений, включая традиционные компьютерные преступления, а также сетевые преступления. Поскольку эти преступления во многом отличаются друг от друга, не существует единого критерия, который может включать в себя все действия, упомянутые в проекте Стэнфордской конвенции и Конвенции о киберпреступности, исключая при этом традиционные преступления, которые совершаются с использованием только оборудования. Тот факт, что не существует единого определения "киберпреступности", не должен быть очень важным до тех пор, пока этот термин не используется в качестве юридического термина[88].

2.2 Типология киберпреступности

Термин "киберпреступность" включает в себя большое разнообразие преступлений[89]. Признанные преступления охватывают широкий спектр правонарушений, что усложняет разработку системы типологии или классификации для киберпреступности[90]. Одна интересная система приводится в Конвенции о киберпреступности Совета Европы[91]. Конвенция о киберпреступности различает четыре типа правонарушений[92]:

- Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем[93];
- Преступления, связанные с компьютерами[94];
- Преступления, связанные с контентом[95]; и
- Преступления, связанные с правами собственности[96].

---

86 Article 4 – Data Interference:
(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
(2) A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

87 For difficulties related to the application of cybercrime definition to real-world crimes see: Brenner, Cybercrime Metrics: Old Wine, New Bottles?, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: http://www.vjolt.net/vol9/issue4/v9i4_a13-Brenner.pdf.

88 In civil law countries, the use of such a legal term could lead to conflicts with the principle of certainty.

89 Some of the most well known cybercrime offences are illegal access, illegal interception of computer data, data interference, computer-related fraud, computer-related forgery, dissemination of child pornography. For an overview see: *Sieber*, Council of Europe Organised Crime Report 2004; ABA International Guide to Combating Cybercrime, 2002; *Williams*, Cybercrime, 2005, in Miller, Encyclopaedia of Criminology.

90 *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Chawki,* Cybercrime in France: An Overview, 2005, available at: http://www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: http://www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf.

91 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http;//conventions.coe.int. Regarding the Convention on Cybercrime see: *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq*.; *Gercke*, National, Regional and International Aproaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seqq; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol 95, No.4, 2001, page 889 *et seq*.

92 The same typology is used by the ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008. The report is available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

93 Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices). For more information about the offences see below: Chapter 6.1.

94 Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences see below: Chapter 6.1.

95 Art. 9 (Offences related to child pornography). For more information about the offences see below: Chapter 6.1.

96 Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences see below: Chapter 6.1.

Эта типология не является полностью последовательной, поскольку она не основана на едином базовом критерии, который бы определял различия между категориями. Три категории сфокусированы на объекте юридической защиты: "Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем"[97]; преступлениях, связанных с контентом[98]; и преступлениях, связанных с правами собственности[99]. Четвертая категория "преступления, связанные с компьютерами"[100] сфокусирована не на объекте юридической защиты, а на методе. Эта непоследовательность приводит к некоторому пересечению между категориями.

Кроме того, некоторые термины, которые используются для описания преступных действий (например, "кибертерроризм"[101] или "фишинг"[102]), охватывают действия, которые попадают в несколько категорий. Тем не менее, категории, приведенные в Конвенция о киберпреступности, являются полезной основой для обсуждения явления киберпреступности.

2.3 Статистические показатели кибернетических правонарушений

Очень трудно количественно оценить влияние киберпреступности на общество[103]. Финансовые потери, обусловленные киберпреступностью, а также число правонарушений оценить очень трудно. Согласно некоторым источникам, потери из-за киберпреступности для предприятий и организаций в Соединенных Штатах Америки[104] достигают 67 миллиардов долл. США; однако неясно, оправдана ли экстраполяция примерных результатов исследований[105]. Эта методологическая критика применима не только к потерям, но так же и к известным правонарушениям[106].

Трудно измерить число киберпреступлений, поскольку их жертвы могут не всегда сообщать о правонарушениях[107]. Тем не менее, исследования могут помочь в понимании влияния киберпреступности. Более важно, что точное число киберпреступлений в каждый отдельно взятый год – это тенденция, которую можно определить путем сравнения результатов за последние несколько лет.

Одним из примеров является обзор компьютерных преступлений и безопасности 2007 г., выполненный ЦРУ в Соединенных Штатах Америки[108], в котором помимо иных тенденций анализируется число совершенных преступлений, связанных с компьютерами[109]. Оно основано на ответах, полученных от 494 практикующих экспертов в области компьютерной безопасности из корпораций США, правительственных органов и финансовых организаций США[110]. В исследовании задокументировано множество правонарушений, о которых сообщили респонденты с 2000 по 2007 год. В нем показано, что с 2001 года уменьшился процент респондентов, которые испытывали или видели вирусные атаки или несанкционированный доступ к информации, или проникновение в систему. В исследовании не объяснено, почему такое уменьшение происходит. Однако это снижение числа распознанных правонарушений указанных категорий

---

97 See below: Chapter 2.4.
98 See below: Chapter 2.5
99 See below: Chapter 2.6
100 See below: Chapter 2.7
101 See below: Chapter 2.8.1
102 The term “phishing” describes an act that is carried out to make the victim disclose personal/secret information. The term “phishing” originally described the use of e-mails to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.4.
Regarding the legal response to phishing see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 et. seqq.
103 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.
104 See 2005 FBI Computer Crime Survey, page 10 As well as *Evers*, Computer crimes cost $67 billion, FBI says, ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.
105 See below: Chapter 2.9.
106 Regarding the economic impact of Cybercrime see below: Chapter 2.9.
107 “The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office.” See Heise News, 27.10.2007, - available at: http://www.heise-security.co.uk/news/80152.
108 Computer Security Institute (CSI), United States.
109 The CSI Computer Crime and Security Survey 2007 is available at: http://www.gocsi.com/
110 See CSI Computer Crime and Security Survey 2007, page 1, available at: http://www.gocsi.com/. With regard to the composition of the respondents the survey is likely to be relevant for the United States only.

подтверждается также исследованиями других организаций (в противовес тому, что иногда предполагают средства массовой информации)[111]. Аналогичное развитие наблюдается и при анализе статистики преступности, например статистика преступности Германии[112] показывает, что после пика в 2004 г. количество преступлений, связанных с компьютерами, уменьшилось вплоть до уровня 2002 года.

Статистические данные по киберпреступности не позволяют предоставить надежную информацию о масштабе или размерах правонарушений[113]. Эта неуверенность относительно размеров правонарушений, о которых сообщают их жертвы[114], а также факт невозможности найти объяснение снижению уровня киберпреступности, делают эти статистические данные открытыми для различных интерпретаций. В настоящее время нет достаточного числа доказательств, для того чтобы предсказывать будущие тенденции и ход развития.

2.4 Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем

Все преступления в этой категории направлены против как минимум одного из трех юридических принципов конфиденциальности, целостности и готовности. В отличие от преступлений, которые описаны в уголовном законодательстве на протяжении веков, например кража или убийство, компьютеризация правонарушений появилась не так давно, поскольку компьютерные системы и компьютерная информация разработаны примерно шестьдесят лет назад[115]. Для эффективного наказания за такие деяния требуется, чтобы существующие положения уголовного права защищали от незаконных действий не только вещественные предметы и физические документы, но и были расширены таким образом, чтобы они включали в себя эти новые юридические принципы[116]. В данном разделе приводится обзор наиболее часто встречающихся правонарушений, подпадающих под эту категорию.

2.4.1 Незаконный доступ (хакерство, взлом шифра)[117]

Правонарушением, описанным как "хакерство" называют незаконный доступ к компьютерной системе[118], одно из старейших преступлений, связанных с компьютерами[119]. В соответствии с развитием компьютерных сетей (особенно, интернета), это преступление стало массовым явлением[120]. Среди важнейших жертв хакерских атак Национальное управление по аэронавтике и исследованию космического пространства Соединенных Штатов Америки (НАСА), Военно-воздушные силы США, Пентагон, Yahoo, Google, Ebay и правительство Германии[121]. Примеры хакерских правонарушений включают в себя:

---

111 See, for example, the 2005 FBI Computer Crime Survey, page 10.

112 See Polizeiliche Kriminalstatisik 2006, available at: http://www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

113 With regard to this conclusion, see as well: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22, available at: http://www.gao.gov/new.items/d07705.pdf. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

114 See below: Chapter 2.9.2.

115 Regarding the development of computer systems, see *Hashagen*, The first Computers – History and Architectures.

116 See in this context for example the Explanatory Report to the Council of Europe Convention on Cybercrime No 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

117 From a legal perspective, there is no real need to differentiate between "computer hackers" and "computer crackers" as – in the context of illegal access – both terms are used to describe persons who enter a computer system without right. The main difference is the motivation. The term "hacker" is used to describe a person who enjoys exploring the details of programmable systems, without breaking the law. The term "cracker" is used to describe a person who breaks into computer systems in general by violating the law.

118 In the early years of IT development, the term "hacking" was used to describe the attempt to get more out of a system (software or hardware) than it was designed for. Within this context, the term "hacking" was often used to describe a constructive activity.

119 See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: http://www.aic.gov.au/publications/htcb/htcb005.pdf.; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61.

120 See the statistics provides by HackerWatch. The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 et. seq. in the month of August 2007. Source: http://www.hackerwatch.org.

121 For an overview of victims of hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sq.; Regarding the impact see *Biegel,* Beyond our Control? The Limits of our Legal System in the Age of Cyberspace, 2001, page 231 et. seq.

- Взлом защищенных паролями веб-сайтов[122]; и
- Обход парольной защиты компьютера.

Примеры подготовительных действий включают в себя:

- Использование неисправного оборудования или программных реализаций для незаконного получения пароля для входа в компьютерную систему[123];
- Создание "подставных" веб-сайтов, для того чтобы заставить пользователей раскрыть свои пароли[124] и
- Установка аппаратных и программных методов регистрации нажатий клавиш на клавиатуре (например, "клавиатурный шпион"), которые записывают каждое нажатие клавиш и, следовательно, любые пароли, используемые на компьютере и/или устройстве[125].

Рисунок 1

На этом рисунке показан веб-сайт, который был взломан. Нарушитель изменил первую страницу, для того чтобы сообщить пользователям об успешной атаке.

Мотивация у правонарушителей различна. Некоторые правонарушители ограничивают свои действия обходом мер безопасности только для того, чтобы доказать свои способности (показано на Рисунке 1[126]). Другие действуют по политическим мотивам, известным как "хактивизм"[127], одним из примеров которого является недавний инцидент, затрагивающий основной веб-сайт Организации Объединенных Наций[128]. В большинстве случаев мотивация у правонарушителей не ограничивается незаконным доступом к компьютерной системе. Правонарушители используют свой доступ для совершения дальнейших преступлений, таких как информационный шпионаж, манипуляция данными, атаки типа "отказ в обслуживании" (DoS)[129]. В большинстве случаев незаконный доступ к компьютерной системе является только необходимым первым шагом[130].

Во многих результатах анализа признается растущее число попыток получить незаконный доступ к компьютерной системе. Только в течение августа 2007 года по всему миру зарегистрировано более 250 миллионов таких случаев[131]. Растущее число хакерских атак обусловлено тремя основными причинами:

Неадекватная и неполная защита компьютерных систем

Сотни миллионов компьютеров присоединены к интернету, и множество компьютерных систем не имеют адекватной защиты для предотвращения незаконного доступа[132]. Анализ, выполненный Университетом Мэриленда, предполагает, что незащищенная компьютерная система, которая присоединена к интернету, испытает на себе атаку менее чем через минуту[133]. Установка мер защиты может снизить риск, но успешные

---

122 *Sieber*, Council of Europe Organised Crime Report 2004, page 65.
123 *Musgrove*, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.
124 *Sieber*, Council of Europe Organised Crime Report 2004, page 66.
125 *Sieber*, Council of Europe Organised Crime Report 2004, page 65. Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.
126 Hacking into a computer system and modifying information on the first page to prove the ability of the offender can – depending on the legislation in place – be prosecuted as illegal access and data interference. For more information, see below Chapter 6.1.a and Chapter 6.1.d.
127 The term “Hacktivism” combines the words hack and activism. It describes hacking activities performed to promote a political ideology. For more information, see: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf; Regarding cases of political attacks see: *Vatis*, cyberattacks during the war on terrorism: a predictive analysis, available at: http://www.ists.dartmouth.edu/analysis/cyber_a1.pdf.
128 A hacker left messages on the website that accused the United States and Israel of killing children. For more information, see BBC News, “UN's website breached by hackers”, available at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6943385.stm
129 The abuse of hacked computer systems often causes difficulties for law enforcement agencies, as electronic traces do not often lead directly to the offender, but first of all to the abused computer systems.
130 Regarding different motivations and possible follow up acts see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1;
131 The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported in the month of August 2007. Source: http://www.hackerwatch.org.
132 Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5.
133 See Heise News, Online-Computer werden alle 39 Sekunden angegriffen, 13.02.2007, available at: http://www.heise.de/newsticker/meldung/85229. The report is based on an analysis from Professor Cukier.

атаки на хорошо защищенные компьютерные системы доказали, что меры технической защиты никогда не смогут полностью остановить атаки[134].

Разработка программных инструментов, которые автоматизируют атаки

В последнее время для автоматизации атак применяются программные инструменты[135]. При помощи программ и атак с заранее установленными параметрами за один день, используя один компьютер, один нарушитель может атаковать тысячи компьютерных систем[136]. Если у нарушителя имеется доступ к большему числу компьютеров, например, при помощи сетевого робота[137], он/она может еще больше увеличить масштаб преступления. Поскольку большая часть программных инструментов используют заранее определенные методы атак, не все атаки оказываются успешными. Пользователи, которые регулярно обновляют свои операционные системы и программные приложения, снижают для себя риск стать жертвой таких широкомасштабных атак, поскольку компании, разрабатывающие защитные программы, анализируют инструменты атаки и готовятся к стандартным хакерским атакам.

Высокоуровневые атаки часто основываются на специально разработанных атаках. Успех этих атак часто обусловлен не применением чрезвычайно сложных методов, а количеством атакуемых компьютерных систем. Инструменты, позволяющие выполнять такие стандартные атаки, широко доступны в интернете[138], некоторые из них бесплатно, но эффективные инструменты могут стоить несколько тысяч долларов США[139]. Одним из примеров является хакерский инструмент, который позволяет правонарушителям определить диапазон IP-адресов (например, от 111.2.0.0 до 111.9.253.253). Эта программа позволяет сканировать все компьютеры в поисках незащищенных портов с использованием одного из этих определенных IP-адресов[140].

Растущая роль частных компьютеров в хакерских стратегиях

Доступ к компьютерной системе часто не является основной мотивацией атаки[141]. Поскольку рабочие компьютеры обычно лучше защищены, чем частные компьютеры, атаки на рабочие компьютеры с использованием заранее сконфигурированных программных инструментов осуществить намного сложнее[142]. В течение последних нескольких лет нарушители все больше нацеливают свои атаки на частные компьютеры, поскольку многие частные компьютеры защищены недостаточно. Более того, частные компьютеры часто содержат ценную информацию (например, о кредитной карте или данные о банковском счете). Правонарушители часто атакуют частные компьютеры потому, что после успешной атаки правонарушитель может включить этот компьютер в свой сетевой робот и использовать его для последующих преступных действий[143].

---

[134] For an overview of examples of successful hacking attacks, see http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.

[135] Regarding threats from Cybercrime toolkits, see Opening Remarks by ITU Secretary-General, 2nd Facilitation Meeting for WSIS Action Line C5, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/sg-opening-remarks-14-may-2007.pdf. See in this context as well: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 29, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[136] For an overview of the tools used, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: http://www.212cafe.com/download/e-book/A.pdf.

[137] Botnets is a short term for a group of compromised computers running programmes that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: http://www.fas.org/sgp/crs/terror/RL32114.pdf; See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

[138] Websense Security Trends Report 2004, page 11, available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security - Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: http://www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[139] For an overview of the tools used, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: http://www.212cafe.com/download/e-book/A.pdf.

[140] *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9, available at: http://www.212cafe.com/download/e-book/A.pdf.

[141] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.250.

[142] For an overview of the tools used to perform high-level attacks, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: http://www.212cafe.com/download/e-book/A.pdf; *Erickson*, Hacking: The Art of Exploitation, 2003.

[143] Botnets is a short term for a group of compromised computers running programmes that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: http://www.fas.org/sgp/crs/terror/RL32114.pdf. For more information about botnets see below: Chapter 3.2.i.

Незаконный доступ к компьютерной системе может считаться аналогичным незаконному доступу в здание и во многих странах признается уголовным преступлением[144]. Анализ различных подходов к судебному преследованию компьютерного доступа показывает, что действующие положения в ряде случаев путают незаконный доступ с последующими правонарушениями или пытаются ограничить судебное преследование незаконного доступа только случаями серьезных нарушений. В некоторых положениях предусмотрено судебное преследование первоначального доступа, а другие считают уголовным преступлением только те случаи, когда:

- система, к которой получен доступ, защищена средствами безопасности[145]; и/или
- нарушитель имел опасные намерения[146]; и/или
- информация была получена, изменена или искажена.

Другие законодательные системы не считают преступлением простой доступ, а фокусируются на последующих правонарушениях[147].

2.4.2 Информационный шпионаж

Ценная информация часто хранится в компьютерных системах. Если компьютерная система соединена с интернетом, правонарушители могут попытаться получить доступ к этой информации через интернет почти из любой точки мира[148]. Интернет все чаще используется для получения коммерческих секретов[149]. Стоимость ценной информации и возможность получить к ней удаленный доступ дает информационный шпионаж чрезвычайно интересным. В 1980-годах ряд немецких хакеров успешно проник в компьютерные системы правительства и обороны Соединенных Штатов Америки, получил секретную информацию и продал эту информацию агентам из Советского Союза[150].

Правонарушители используют различные способы для получения доступа к компьютерам своих жертв[151], включая:

- использование программ для сканирования незащищенных портов[152];
- использование программ для обхода средств защиты153; и
- "психологическая атака"[154].

Особенно интересен последний подход "психологическая атака", который является нетехническим видом проникновения и, главным образом, опирается на взаимодействие между людьми, подразумевает обман других людей с целью разрушения обычных процедур обеспечения безопасности, поскольку он основан не на технических средствах[155]. "Психологическая атака", тем не менее, очень эффективна для атак на хорошо

---

144 See *Schjolberg*, The legal framework - unauthorized access to computer systems – penal legislation in 44 countries, available at: http://www.mosstingrett.no/info/legal.html.

145 See in this context Art. 2, sentence 2 Convention on Cybercrime.

146 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.264.

147 One example of this is the German Criminal Code, that criminalised only the act of obtaining data (Section 202a), until 2007, when the provision was changed. The following text is taken from the old version of Section 202a - Data Espionage:
(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.
(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

148 For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 et seqq. *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotrionte*, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.

149 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage — 2003, page 1, available at: http://www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

150 For more information about that case see: *Stoll*, Stalking the wily hacker, available at: http://pdf.textfiles.com/academics/wilyhacker.pdf; *Stoll*, The Cuckoo's Egg, 1998.

151 See *Sieber*, Council of Europe Organised Crime Report 2004, page 88 et seqq; *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: http://www.212cafe.com/download/e-book/A.pdf.

152 *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 et seqq., available at: http://www.212cafe.com/download/e-book/A.pdf.

153 Examples are software tools that are able to break passwords. Another example is a software tool that records keystrokes (keylogger). Keyloggers are available as software solutions or hardware solutions.

154 See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: http://www.securityfocus.com/infocus/1527.

155 See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

защищенные компьютерные системы. Они еще подробнее описывают манипуляцию людьми при взаимодействии с целью получения доступа к компьютерным системам[156]. Психологическая атака обычно очень успешна, потому что самым слабым звеном в компьютерной безопасности зачастую являются пользователи компьютерных систем.

Например, в последнее время основным преступлением, совершаемым в киберпространстве[157], стал "фишинг". Он характеризуется попытками мошеннического получения ценной информации, например паролей, посредством маскировки под доверенное лицо или предприятие, например финансовую организацию, в процессе кажущейся официальной электронной переписки.

Хотя человеческая уязвимость пользователей открывает ворота риску обмана, она также предлагает и решения. Хорошо образованные пользователи компьютера не являются легкой добычей для правонарушителей. Образование пользователей – важная часть любой стратегии борьбы с киберпреступностью[158]. ОЭСР подчеркивает важность криптографии для пользователей, поскольку криптография может оказать содействие в повышении защиты данных[159]. Если физическое лицо или организация, хранящие информацию, применят соответствующие меры защиты, криптографическая защита может оказаться более эффективной, чем любая физическая защита[160]. Успех действий правонарушителей в получении ценной информации часто обусловлен отсутствием мер защиты.

Хотя правонарушители обычно нацеливаются на производственные секреты, все чаще их целью становятся данные, хранимые на частных компьютерах[161]. Частные пользователи часто хранят на своих компьютерах данные о банковских счетах или кредитных картах[162]. Правонарушители могут использовать эту информацию для собственных целей (например, данные о банковских счетах для выполнения денежных переводов) или продать ее третьей стороне[163]. Записи о кредитных картах, например, продаются за сумму от 60 долл. США[164]. Интересна нацеленность хакеров на частные компьютеры, поскольку выгода от полученных промышленных секретов обычно выше чем выгоды, получаемые в результате получения или продажи информации об одной кредитной карте. Однако, поскольку частные компьютеры обычно защищены хуже, информационный шпионаж, основанный на частных компьютерах, вероятно, станет еще более прибыльным.

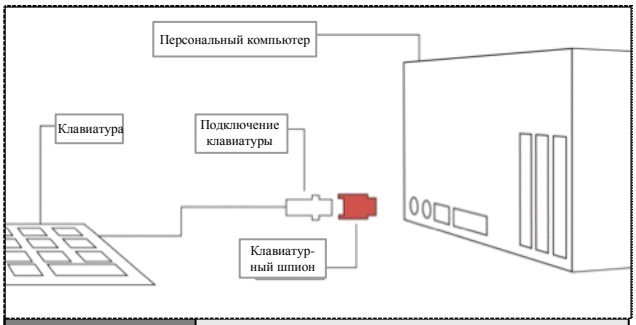


Рисунок 2

На рисунке показано, как устанавливаются аппаратные клавиатурные шпионы. Большая часть таких инструментов, которые выглядят как адаптеры, размещаются между клавиатурой и компьютером. Некоторые последние модели встраиваются в клавиатуру, так что их невозможно найти, не открывая оборудование. Антивирусные программные продукты не могут найти аппаратных клавиатурных шпионов.

Существует два подхода к получению информации:

---

156 For more information, see *Mitnick/Simon/Wozniak*, The Art of Deception: Controlling the Human Element of Security.

157 See the information offered by anti-phishing working group, available at: http://www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: http://www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606; The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

158 Regarding the elements of an Anti-Cybercrime Strategy, see below: Chapter 4.

159 "Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems" - See OECD Guidelines for Cryptography Policy, V 2, available at: http://www.oecd.org/document/11/0,3343,en_2649_34255_1814731_1_1_1_1,00.html.

160 Physical researches prove that it can take a very long time to break encryption, if proper technology is used. See *Schneier*, Applied Cryptography, page 185. For more information regarding the challenge of investigating Cybercrime cases that involve encryption technology, see below: Chapter 3.2.m.

161 Regarding the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 et seqq.

162 Regarding the impact of this behaviour for identity-theft see *Gercke*, Internet-related Identity Theft, 2007, available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf

163 *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.

164 See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

- получение доступа к компьютерной системе или хранилищу данных и получения информации; или
- использование различных манипуляций, для того чтобы заставить пользователей раскрыть информацию или коды доступа, которые помогут правонарушителям получить доступ к информации ("фишинг").

Правонарушители часто используют компьютерные инструменты, установленные на компьютерах жертв, или вредоносные программы, называющиеся шпионскими программами, для передачи данных на них[165]. В течение последних десяти лет обнаружены различные типы шпионских программ, например "клавиатурные шпионы"[166]. Клавиатурные шпионы – это программные инструменты, который регистрируют каждое нажатие клавиш на клавиатуре зараженного компьютера[167]. Эти же клавиатурные шпионы передают всю записанную информацию правонарушителю, как только компьютер выйдет в интернет. Другие выполняют первоначальную сортировку и анализ записанных данных, например, фокусируясь на потенциальной информации о кредитных картах[168], для передачи любой полученной ценной информации.

Аналогичные устройства представлены также как аппаратные устройства, которые подключаются между клавиатурой и компьютерной системой для записи нажатий на клавиши клавиатуры (см. Рисунок 4). Аппаратные клавиатурные шпионы намного сложнее установить и обнаружить, поскольку требуется физический доступ к компьютерной системе[169]. Однако классическое антишпионские и антивирусные программы, как правило, не способны их обнаружить[170].

Помимо доступа к компьютерным системам правонарушители могут получать данные путем манипулирования пользователями. В последнее время правонарушители разработали эффективные методы обмана для получения секретной информации, например, данные о банковском счете или кредитной карте, путем управления пользователем при помощи методов психологической атаки[171]. В последнее время "фишинг" стан одним из наиболее значительных преступлений в киберпространстве[172]. Термин "фишинг" используется для описания типа преступлений, который характеризуется попытками мошеннического получения ценной информации, например паролей, выдавая себя за доверенное лицо или предприятие (например, финансовую организацию) в процессе электронного взаимодействия, которое выглядит как официальное[173].

Информационный шпионаж – это еще один вид преступлений, который хитроумно направлен на одно из наиболее слабых звеньев компьютерной безопасности пользователя. Учитывая это, явно видны риски, которые появляются вместе с этими видами обмана. Но такое положение дел также позволяет найти и решения. Хорошо образованные пользователи компьютера не являются легкой добычей для правонарушителей. Это подчеркивает важность образования пользователей, как важнейшей части любой стратегии по борьбе с киберпреступностью[174].

Ценная информация все чаще хранится в компьютерных системах. Очень важно оценить, являются ли адекватными предпринимаемые пользователем меры технической защиты, или законодатели должны установить дополнительную защиту, объявляя информационный шпионаж незаконным деянием[175].

2.4.3 Незаконный перехват

Правонарушители могут перехватывать переписку между пользователями[176], например электронные письма, или перехватывать передачу данных (когда пользователи загружают данные на веб-севера или заходят на внешние средства хранения на базе веб-технологии[177]) для записи передаваемой информации.

---

[165] See *Hackworth*, Sypware, Cybercrime & Security, IIA-4. Regarding user reactions to the threat of spyware, see: Jaeger/ Clarke, "The Awareness and Perception of Spyware amongst Home PC Computer Users", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Jaeger%20Clarke%20-%20The%20Awareness%20and%20Perception%20of%20Spyware%20amongst%20Home%20PC%20Computer%20Users.pdf.

[166] See *Hackworth*, Sypware, Cybercrime & Security, IIA-4, page 5.

[167] For further information about keyloggers, see: http://en.wikipedia.org/wiki/Keylogger; Netadmintools Keylogging , available at: http://www.netadmintools.com/part215.html

[168] It is easy to identify credit card numbers, as they in general contain 16 numbers. By excluding phone numbers using country codes, offenders can identify credit card numbers and exclude mistakes to a large extent.

[169] One approach to gain access to a computer system to install a key-logger is например to gain access to the building where the computer is located using social engineering techniques e.g., a person wearing a uniform from the fire brigade pretending to check emergency exits has a good chance of gaining access to a building, if more extensive security is not in place. Further approaches can be found in *Mitnick*, "The Art of Deception: Controlling the Human Element of Security", 2002.

[170] Regular hardware checks are a vital part of any computer security strategy.

[171] See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: http://www.securityfocus.com/infocus/1527.

[172] See the information offered by anti-phishing working group, available at: http://www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: http://www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606.

[173] For more information on the phenomenon of phishing see below: Chapter 2.8.4.

[174] Regarding the elements of an Anti-Cybercrime Strategy see below: Chapter 4.

[175] The Council of Europe Convention on Cybercrime contains no provision criminalising data espionage.

[176] *Leprevost*, "Encryption and cryptosystems in electronic surveillance: a survey of the technology assessment issues", Development of surveillance technology and risk of abuse of economic information, 2.4, available at: http://cryptome.org/stoa-r3-5.htm.

[177] With the fall in price of server storage space, the external storage of information has become more popular. Another advantage of

Правонарушители могут иметь своей целью любую инфраструктуру связи, например, фиксированные или беспроводные каналы и любые услуги интернета, например, электронную почту, чаты или связь VoIP[178].

Большая часть передачи данных через инфраструктуру поставщиков доступа в интернет или поставщиков услуг интернета хорошо защищена, и их трудно перехватить[179]. Однако правонарушители ищут слабые точки в системе. Беспроводные технологии приобрели большую популярность и в прошлом показали свою уязвимость[180]. Сегодня отели, рестораны и бары предлагают своим клиентам доступ в интернет через беспроводные точки доступа. Однако сигналы передачи данных между компьютером и точкой доступа могут быть приняты в радиусе до 100 метров[181]. Правонарушители, желающие перехватить процесс обмена данными, могут сделать это из любой точки в пределах этого радиуса (Рисунок 3). Даже в том случае, когда беспроводная передача зашифрована, правонарушители могут иметь возможность дешифровать записанную информацию[182].

Для получения доступа к ценной информации некоторые правонарушители устанавливают точки доступа вблизи мест, где имеется большой спрос на беспроводной доступ[183] (например, вблизи баров и гостиниц). Местоположение станции часто имеет такое название, чтобы пользователи, ищущие точку доступа в интернет, с большей вероятностью остановили свой выбор на мошеннической точке доступа. Если пользователи доверяют поставщику услуг доступа в деле обеспечения безопасности своей связи без применения собственных мер безопасности, то правонарушители смогут легко перехватить передачу.

Использование фиксированных линий не мешает правонарушителям перехватывать передачи[184]. Во время передачи данных по проводам излучается электромагнитная энергия[185]. Если правонарушители используют соответствующее оборудование, они могут обнаружить и записать эти передачи[186] и смогут записать передачу данных между компьютерами пользователей и системой, к которой они присоединены, и также внутри компьютерной системы[187].

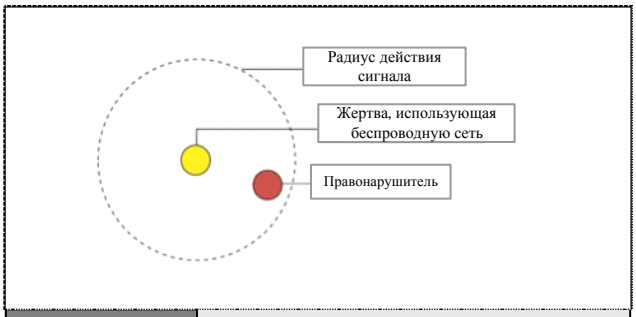


Рисунок 3

На рисунке показан сценарий атаки на пользователя компьютером, использующего беспроводное сетевое соединение. Правонарушитель, желающий перехватить передачу, может действовать из любой точки в пределах радиуса действия сигнала. В зависимости от точки размещения беспроводного маршрутизатора, сигналы могут быть приняты в радиусе до 100 метров.

Большинство стран защищает услуги связи путем судебного преследования незаконного перехвата телефонных переговоров. Однако учитывая растущую популярность услуг на базе протокола IP, законодателям необходимо оценить, до какой степени аналогичная защита может быть обеспечена в услугах на базе протокола IP[188].

---

external storage is that information can be accessed from every Internet connection.

178 Regarding the interception of VoIP to assist law enforcement agencies, see *Bellovin and others*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf; Regarding the potential of VoIP and regulatory issues see: *Braverman*, VoIP: The Future of Telephony is now…if regulation doesn"t get in the way, The Indian Journal of Law and Technology, Vol.1, 2005, page 47 et seq., available at: http://www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf.

179 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 30, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

180 *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime" in Cybercrime & Security, IIA-2, page 6 et seq.

181 The radius depends on the transmitting power of the wireless access point. See http://de.wikipedia.org/wiki/WLAN.

182 With regard to the time necessary for decryption see below: Chapter 3.2.13.

183 Regarding the difficulties in Cybercrime investigations that include wireless networks, see *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime" " in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: http://www.aic.gov.au/publications/tandi2/tandi329t.html.

184 *Sieber*, Council of Europe Organised Crime Report 2004, page 97.

185 With regard to the interception of electromagnetic emissions see: Explanatory Report to the Convention on Cybercrime, No. 57.

186 See http://en.wikipedia.org/wiki/Computer_surveillance#Surveillance_techniques.

187 E.g. the electromagnetic emission caused by transmitting the information displayed on the screen from the computer to the screen.

188 For more details on legal solutions see below: Chapter 6.1.3.

2.4.4 Искажение информации

Компьютерная информация жизненно важна для частных пользователей, предприятий и администраций, все они зависят от целостности и доступности данных[189]. Отсутствие доступа к данным может привести к существенным финансовым потерям. Правонарушители могут нарушить целостность данных и исказить их при помощи[190]:

- удаления данных; и/или
- блокировки данных; и/или
- изменения данных; и/или
- ограничения доступа к ним.

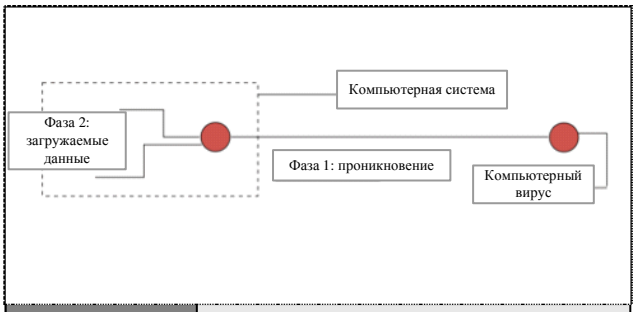


Рисунок 4

На рисунке показано действие компьютерного вируса. После заражения компьютерной системы (фаза 1) вирус выполняет загрузку программы (фаза 2). Это может, например, быть удалением или шифрованием определенных файлов.

Одним из распространенных примеров удаления данных является компьютерный вирус[191]. С самого начала развития компьютерных технологий компьютерные вирусы угрожали пользователям, которые не установили соответствующую защиту[192]. С тех пор количество компьютерных вирусов значительно увеличилось[193]. Две недавних важнейших разработки предусматривают изменения в:

- пути распространения вирусов; и
- загружаемых данных[194].

Ранее компьютерные вирусы распространялись через устройства хранения данных, такие как гибкие диски, тогда как теперь большая часть вирусов распространяется через интернет в виде приложений либо к электронным письмам, либо к файлам, которые пользователи загружают из интернета[195]. Эти новые эффективные методы распространения намного усилили вирусное заражение и существенно повысили число зараженных компьютерных систем. По оценкам, компьютерный червь SQL Slammer[196] заразил 90% уязвимых компьютерных систем за первые 10 минут своего распространения[197]. Финансовый урон, обусловленный вирусными атаками только за 2000 год, оценен величиной порядка 17 миллиардов долл. США.[198] В 2003 году он все еще превышал 12 миллиардов долл. США[199].

Большинство компьютерных вирусов первого поколения либо удаляли информацию, либо отображали сообщение (см. Рисунок 4). В последнее время загружаемые данные стали разнообразными.[200]

---

189 See in this context as well: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 32, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

190 *Sieber*, Council of Europe Organised Crime Report 2004, page 107.

191 A computer virus is software that is able to replicate itself and infect a computer, without the permission of the user to harm the computer system. See *Spafford*, "The Internet Worm Program: An Analysis", page 3; *Cohen*, "Computer Viruses - Theory and Experiments", available at: http://all.net/books/virus/index.html. *Cohen*, "Computer Viruses"; *Adleman*, "An Abstract Theory of Computer Viruses". Regarding the economic impact of computer viruses, see *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12; Symantec "Internet Security Threat Report", Trends for July-December 2006, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

192 One of the first computer virus was called (c)Brain and was created by *Basit* and *Amjad Farooq Alvi*. For further details, see: http://en.wikipedia.org/wiki/Computer_virus.

193 *White/Kephart/Chess*, Computer Viruses: A Global Perspective, available at: http://www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib.html.

194 Payload describes the function the virus performs after it is installed on victims" computers and activated. Examples of the payload are: Displaying messages or performing certain activities on computer hardware such as opening the CD drive or deleting or encrypting files.

195 Regarding the various installation processes see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 21 et seq., available at: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

196 See BBC News, "Virus-like attack hits web traffic", 25.01.2003, http://news.bbc.co.uk/2/hi/technology/2693925.stm;

197 Critical Infrastructure Protection Department Of Homeland Security Faces Challenges In Fulfilling Cybersecurity Responsibilities, GAO, 2005 GAO-05-434, page 12, available at: http://www.gao.gov/new.items/d05434.pdf.

198 *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12, available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

199 *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12, available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf.

200 See *Szor*, The Art of Computer Virus Research and Defence, 2005.

Современные вирусы способны устанавливать потайные входы, позволяющие правонарушителям дистанционно управлять компьютером жертвы или шифровать файлы так, чтобы у жертвы не могли получить доступ к собственным файлам, пока они не заплатят за ключ[201].

2.4.5 Искажения системы

Те же самые вопросы, вызывающие озабоченность в связи с атаками на компьютерные данные, относятся и к атакам на компьютерные системы. Большинство организаций используют интернет-услуги в процессе производства, что позволяет иметь готовность 24 часа в сутки и доступность по всему миру[202]. Если правонарушители сумеют нарушить беспрерывность работы компьютерных систем, это может привести к большим финансовым потерям у их жертв[203].

Атаки могут выполняться путем физического нападения на компьютерную систему[204]. Если нарушители сумеют получить доступ к компьютерной системе, они смогут разрушить аппаратуру. В большинстве уголовных законодательств дела о дистанционном воздействии не являются существенной проблемой, так как они аналогичны классическим делам о повреждении или разрушении собственности. Однако для высокодоходных предприятий электронной коммерции финансовый урон, наносимый атаками на компьютерную систему, часто намного выше чем просто стоимость компьютерного оборудования[205].

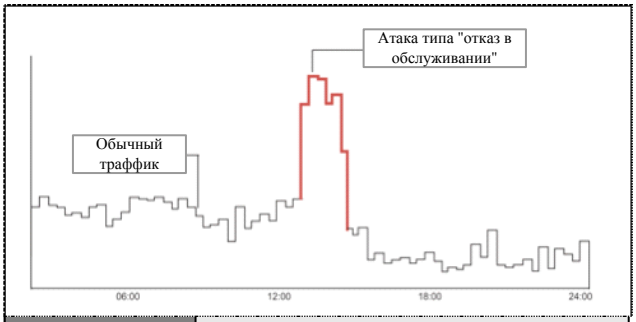


Рисунок 5

График показывает количество запросов доступа к веб-сайту во время нормальной работы (черный цвет) и во время атаки "отказ в обслуживании" (DoS). Если атакуемые услуги не могут справится с возросшим числом запросов, эта атака может замедлить скорость реакции веб-сайта или совсем остановить обслуживание.

Наиболее сложными для законодательства являются обманы на базе веб-технологий. Примеры таких дистанционных атак на компьютерные системы включают в себя:

- компьютерные черви[206]; или
- атаки типа "отказ в обслуживании" (DoS[207]).

Компьютерные черви[208] – это подгруппа вредоносных программ (типа компьютерных вирусов). Компьютерные черви – это самовоспроизводящиеся компьютерные программы, которые наносят вред сети, инициируя множество процессов передачи данных. Они могут влиять на компьютерные системы следующим образом:

---

201 One example of a virus that encrypts files is the Aids Info Disk or PC Cyborg Trojan. The virus hid directories and encrypted the names of all files on the C-drive. Users were asked to 'renew their license' and contact PC Cyborg Corporation for payment. For more information, see: *Bates*, "Trojan Horse: AIDS Information Introductory Diskette Version 2.0" in *Wilding/Skulason*, Virus Bulletin, 1990, page 3..

202 In 2000 a number of well known United States e-Commerce businesses were targeted by denial of service attacks. A full list of the attacks business is provided by *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", page 4, available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.For more information see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq; Lemos, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; Paller, "Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security", Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

203 Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market", Journal of Computer Security, Vol. 11, page 431-448.

204 Examples include: Inserting metal objects in computer devices to cause electrical shorts, blowing hairspray into sensitive devices or cutting cables. For more examples, see *Sieber*, "Council of Europe Organised Crime Report 2004", page 107.

205 Regarding the possible financial consequences, see: *Campbell/Gordon/Loeb/Zhou*, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market", Journal of Computer Security, Vol. 11, page 431-448.

206 *Sieber*, "Council of Europe Organised Crime Report 2004", page 107.

207 A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, "Analysis of a Denial of Service Attack on TCP"; Houle/Weaver, "Trends in Denial of Service Attack Technology", 2001, available at: http://www.cert.org/archive/pdf/DoS_trends.pdf.

208 The term "worm" was used by *Shoch/Hupp*, "The "Worm" Programs – Early Experience with a Distributed Computation", published in 1982. This publication is available for download: http://vx.netlux.org/lib/ajm01.html. With regard to the term "worm", they refer to the science-fiction novel, "The Shockwave Rider" by John Brunner, which describes a programme running loose through a computer network.

- В зависимости от того, что загружается при помощи компьютерного червя, заражение может остановить беспрерывное выполнение операций компьютерной системы и использовать ресурсы системы для самовоспроизведения в интернете.
- Создание трафика в сети может закрыть доступность определенных услуг, например веб-сайтов.

В то время как компьютерные черви, как правило, заражают всю сеть, не имея целью определенные компьютерные системы, атаки DoS нацелены на конкретные компьютерные системы. Атака DoS делает ресурсы компьютера недоступными для легальных пользователей[209]. Направляя на некоторую компьютерную систему большее число запросов, чем эта компьютерная система способна обслужить (см. Рисунок 7), правонарушители могут не дать пользователям возможности получить доступ к компьютерной системе, проверить электронную почту, прочесть новости, заказать авиабилет или загрузить файлы. В 2000 году в течение короткого промежутка времени было совершено несколько атак DoS на такие известные компании как CNN, Ebay и Amazon[210]. В результате некоторые услуги оказались недоступными в течение нескольких часов и даже дней[211].

Наказание за атаки DoS и атаки с использованием компьютерных червей ставят сложные задачи перед большей частью уголовных правовых систем, поскольку эти атаки могут не приводить к физическому повреждению компьютерных систем. Помимо обычной необходимости судебного преследования атак на базе веб-технологий[212], обсуждается вопрос о том, требуется ли отдельный законодательный подход к наказанию за атаки на важнейшую инфраструктуру.

2.5 Преступления, связанные с контентом

К этой категории относится контент, который считается незаконным, включая детскую порнографию, ксенофобные материалы или оскорбления в адрес религиозных символов[213]. Разработка правовых инструментов для борьбы с этой категорией преступлений испытывает более сильное влияние со стороны национальных подходов, которые могут учитывать фундаментальные культурные и правовые принципы. В том, что касается запрещенного содержания, системы оценки и законодательные системы в различных обществах существенно различаются. Распространение ксенофобных материалов является незаконным во многих европейских странах[214], но может защищаться принципами свободы слова[215] в Соединенных Штатах[216]. Использование

---

[209] For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, "Analysis of a Denial of Service Attack on TCP".

[210] See *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension", in Sofaer/Goodman, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 14, available at: http://media.hoover.org/documents/0817999825_1.pdf. The attacks took place between 07.02.2000 and 09.02.2000. For a full list of attacked companies and the dates of the attacks, see: *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", page 4, available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.

[211] *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq; Lemos, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html;

[212] Regarding the different approaches see below: Chapter 6.1.5.

[213] For reports on cases involving illegal content, see *Sieber*, "Council of Europe Organised Crime Report 2004", page 137 et seqq.

[214] One example of the wide criminalisation of illegal content is Sec. 86a German Penal Code. The provision criminalises the use of symbols of unconstitutional parties: Section 86a: Use of Symbols of Unconstitutional Organizations
(1) Whoever: 1. domestically distributes or publicly uses, in a meeting or in writings (Section 11 subsection (3)) disseminated by him, symbols of one of the parties or organizations indicated in Section 86 subsection (1), nos. 1, 2 and 4; or 2. produces, stocks, imports or exports objects which depict or contain such symbols for distribution or use domestically or abroad, in the manner indicated in number 1, shall be punished with imprisonment for not more than three years or a fine.
(2) Symbols, within the meaning of subsection (1), shall be, in particular, flags, insignia, uniforms, slogans and forms of greeting. Symbols which are so similar as to be mistaken for those named in sentence 1 shall be deemed to be equivalent thereto.
(3) Section 86 subsections (3) and (4), shall apply accordingly.

[215] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

пренебрежительных замечаний в адрес пророка Мухаммеда является преступлением во многих арабских странах[217], но не является таковым в некоторых европейских странах.

Эти правовые проблемы сложны, потому что информация, распространяемая с компьютера одного пользователя в одной стране, может быть доступна почти из любой точки мира[218]. Если "правонарушители" создают контент, который является незаконным в некоторых странах, но не в той стране, откуда они работают, наказать этих "правонарушителей" трудно или невозможно[219].

Гораздо более удачно обстоит дело с соглашением относительно содержания материала и относительно степени, до которой конкретные действия подлежат судебному преследованию. Различные национальные взгляды и трудности в наказании преступлений, совершаемых за пределами страны, в которой ведется расследование, вносят свой вклад в блокирование распространения определенных типов контента в интернете. Там, где существует соглашение, запрещающее доступ к веб-сайтам с запрещенным содержанием, размещенным за пределами страны, государства могут иметь строгие законы, блокировать веб-сайты и фильтровать контент[220].

Существуют различные подходы к созданию систем фильтрации. Одно из решений требует, чтобы поставщики устанавливали программы, анализирующие посещаемые веб-сайты, и блокировали веб-сайты, занося их в черный список[221]. Другим решением является установка фильтрующих программ на компьютеры пользователей (удобное решение для родителей, желающих контролировать содержание, которое могут видеть их дети, а также для библиотек и интернет терминалов общего пользования[222]).

Попытки контролировать контент в интернете не ограничиваются определенными типами контента, которые считаются незаконными. В некоторых странах технологию фильтрации используют для ограничения доступа на веб-сайты, где рассматриваются политические вопросы. Инициатива OpenNet[223] сообщает, что в настоящее время цензура применяется примерно в двадцати странах[224].

2.5.1 Эротические или порнографические материалы (за исключением детской порнографии)

Материалы сексуального содержания были одними из первых видов контента, который стал коммерчески распространяться по интернету и который был выгоден для розничных торговцев материалами эротического или порнографического содержания, включая:

- передачу содержания (картинок, фильмов, прямых репортажей) без необходимости использовать дорогостоящие методы доставки[225];
- всемирный[226] доступ, достигающий намного большего числа потребителей, чем магазины розничной продажи;

---

[216] Concerns over freedom of expression (e.g. the First Amendment to the United States Constitution) explain why certain acts of racism were not made illegal by the Convention on Cybercrime, but their criminalisation was included in the First Additional Protocol. See Explanatory Report to the First Additional Protocol, No. 4.

[217] See e.g. Sec. 295C of the Pakistan Penal Code:
295-C. Use of derogatory remarks, etc., in respect of the Holy Prophet: Whoever by words, either spoken or written, or by visible representation or by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Muhammad (peace be upon him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

[218] See below: Chapter 3.2.6 and Chapter 3.2.7.

[219] In many cases, the principle of dual criminality hinders international cooperation.

[220] Regarding filter obligations/approaches see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. seq., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion about filtering in different countries see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: http://www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: http://www.ip-watch.org/weblog/index.php?p=842; Zwenne, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at:
http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at:
http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf; Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

[221] Regarding this approach, see: *Stadler*, Multimedia und Recht 2002, page 343 et seq.; *Mankowski*, Multimedia und Recht 2002, page 277 et seq.

[222] See *Sims*, "Why Filters Can't Work", available at: http://censorware.net/essays/whycant_ms.html; *Wallace*, "Purchase of blocking software by public libraries is unconstitutional", available at: http://censorware.net/essays/library_jw.html.

[223] The OpenNet Initiative is a transatlantic group of academic institutions that reports on internet filtering and surveillance. Harvard Law School and the University of Oxford participate in the network, among others. For more information, see: http://www.opennet.net.

[224] *Haraszti*, Preface, in "Governing the Internet Freedom and Regulation in the OSCE Region", available at:
http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[225] Depending on the availability of broadband access.

[226] Access is in some countries is limited by filter technology. [226] Regarding filter obligations/approaches see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa

- интернет часто считается анонимной средой передачи, что часто является ошибочным[227] – это аспект, который в силу доминирующих взглядов общества очень привлекателен для потребителей порнографии.

В ходе недавних исследований было найдено до 4,2 миллиона веб-сайтов, к которым в любое время можно получить доступ через интернет[228]. Кроме веб-сайтов, порнографические материалы могут распространяться посредством:

- передачи с использованием систем обмена файлами[229];
- передачи в закрытых комнатах чата.

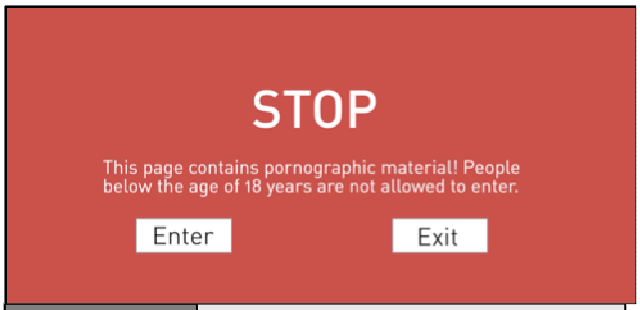


Рисунок 6

На рисунке показан один из подходов, используемых для предотвращения доступа малолетних на веб-сайты с порнографическим содержанием. Поскольку такое решение не обеспечивает проверки ответа, данного пользователем, во многих странах оно считается неадекватным.

В различных странах материалы эротического и порнографического содержания считаются незаконными до различной степени. В некоторых странах разрешен обмен порнографическими материалами между взрослыми и преступлением считаются случаи, когда доступ к материалам такого типа получают дети[230], стремясь защитить молодежь[231]. Исследования показывают, что доступ детей к порнографическим материалам может негативно сказаться на их развитии[232]. Для того чтобы обеспечить выполнение этого закона, были заработаны системы "подтверждения взрослости" (см. Рисунок 6[233]). В других странах преступлением считается любой обмен порнографическими материалами даже между взрослыми[234], без специального внимания к отдельным группам населения, например молодежи.

В странах, где преступлением считается взаимодействие с порнографическими материалами, стоит проблема предотвращения доступа к порнографическим материалам. Помимо интернета, власти часто могут считать и наказывать нарушения запрета на порнографические материалы. Однако, поскольку в интернете порнографические материалы легко доступны с серверов, находящихся за пределами страны, обеспечить выполнение этих законов трудно. Даже там, где власти смогут определить веб-сайты, содержащие

Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. seq ., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion about filtering in different countries see: *Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: http://www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: http://www.ip-watch.org/weblog/index.php?p=842; Zwenne, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement , available at: http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf; Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

227 With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: Chapter 6.2.

228 *Ropelato*, "Internet Pornography Statistics", available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

229 About a third of all files downloaded in file-sharing systems contained pornography. *Ropelato*, "Internet Pornography Statistics", available at: http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html.

230 One example for this approach can be found in Sec. 184 German Criminal Code (Strafgesetzbuch):
Section 184 Dissemination of Pornographic Writings
(1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):
1. offers, gives or makes them accessible to a person under eighteen years of age; […]

231 Regarding this aspect see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 36, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

232 See: *Nowara/Pierschke*, Erzieherische Hilfen fuer jugendliche Sexual(straf)taeter, Katamnesestudie zu den vom Land Nordrhein-Westfalen gefoerterten Modellprojekten, 2008.

233 See *Siebert*, "Protecting Minors on the Internet: An Example from Germany", in "Governing the Internet Freedom and Regulation in the OSCE Region", page 150, available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

234 One example is the 2006 Draft Law, "Regulating the protection of Electronic Data and Information and Combating Crimes of Information" (Egypt): Sec. 37: Whoever makes, imitates, obtains, or possesses, for the purpose of distribution, publishing, or trade, electronically processed pictures or drawings that are publicly immoral, shall be punished with detention for a period not less than six months, and a fine not less than five hundred thousand Egyptian pounds, and not exceeding seven hundred thousand Egyptian pounds, or either penalty.

порнографические материалы, у них может не оказаться сил предотвратить доступ поставщиков услуг к запрещенному контенту.

Принцип *национального суверенитета*, обычно, не позволяет одной стране вести расследования на территории другой страны без разрешения местных властей[235]. Даже, когда власти запрашивают поддержку от стран, в которых располагаются веб-сайты нарушителей, успех расследования и санкции против преступлений могут быть блокированы принципом "обоюдного признания соответствующего деяния преступлением"[236]. Для того чтобы предотвратить доступ к материалам порнографического содержания, страны с особенно строгими законами часто ограничиваются превентивными мерами, например, технологией фильтрации[237]), для ограничения доступа к определенным веб-сайтам[238].

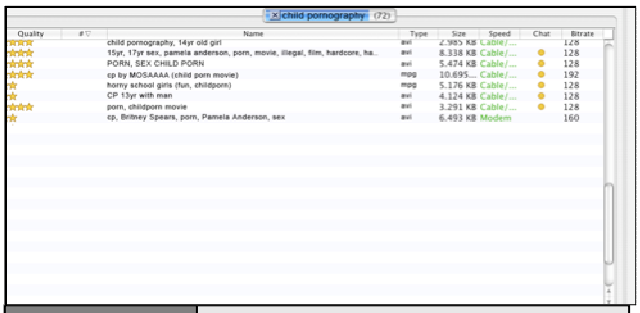


Рисунок 7

На рисунке показан интерфейс пользователя программного обеспечения для обмена файлами. После того, как был передан запрос по словам "детская порнография", программа перечисляет все файлы, загруженные пользователями этой системы обмена файлами и содержат эти слова.

2.5.2 Детская порнография

В отличие от различных взглядов на взрослую порнографию, детская порнография повсеместно преследуется, и правонарушения, связанные с детской порнографией, считаются преступными деяниями[239]. В борьбе против онлайновой детской порнографии участвуют международные организации[240], и существует несколько международных правовых инициатив, включая, помимо прочего, Конвенцию Организации Объединенных Наций 1989 года по правам детей[241]; Рамочное решение Совета Европейского союза 2003 года по борьбе с сексуальной эксплуатацией детей и детской порнографией[242]; и Конвенцию Совета Европы 2007 года о защите детей от сексуальной эксплуатации и сексуальной агрессии[243].

---

235 National Sovereignty is a fundamental principle in International Law. See Roth, 'state Sovereignty, International Legality, and Moral Disagreement", 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

236 Regarding the principle of "dual criminality", see below: Chapter 6.3.2.

237 Regarding technical approaches in the fight against Obscenity and Indecency on the Internet see: Weekes, Cyber-Zoning a Mature Domain: The Solution to Preventing Inadvertent Access to Sexually Explicit Content on the Internet, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: http://www.vjolt.net/vol8/issue1/v8i1_a04-Weekes.pdf.

238 Regarding filter obligations/approaches see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. Seq., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion about filtering in different countries see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: http://www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: http://www.ip-watch.org/weblog/index.php?p=842; Zwenne, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf; Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

239 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

240 See for example the "G8 Communique", Genoa Summit, 2001, available at: http://www.g8.gc.ca/genoa/july-22-01-1-e.asp.

241 United Nations Convention on the Right of the Child, A/RES/44/25, available at: http://www.hrweb.org/legal/child.html. Regarding the importance for Cybercrime legislation see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 35, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

242 Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

243 Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http:// http://conventions.coe.int.

К сожалению, как оказалось, эти инициативы, пытающиеся контролировать сетевое распространение порнографии, очень мало пугают нарушителей, которые используют интернет для передачи и обмена детской порнографией (см. Рисунок 7[244]). Рост пропускной способности позволяет передачу фильмов и архивов изображений.

Исследование поведения правонарушителей в области детской порнографии показывает, что 15% арестованы за наличие у них детской порнографии, связанной с интернетом, имели в своем компьютере более 1000 изображений; у 80% в компьютерах были изображения детей от 6 до 12 лет[245]; у 19% были изображения детей младше 3 лет[246]; и у 21% были картинки, изображающие насилие[247].

Торговля детской порнографией чрезвычайно прибыльна[248], собиратели готовы платить большие суммы за фильмы и изображения, на которых показаны сексуальные сцены с детьми[249]. Поисковые машины быстро отыскивают такие материалы[250]. Большая часть материалов распространяется на закрытых форумах, защищенных паролями, к которым редко имеют доступ обычные пользователи и органы правопорядка. Таким образом, в борьбе с детской порнографией жизненно важны секретные действия[251].

Два главных фактора использования ИКТ для передачи материалов с детской порнографией представляют трудности для расследования этих преступлений:

1 Использование виртуальных денег и анонимные платежи[252]

Оплата наличными позволяет покупателям некоторых товаров скрыть свои данные. Поэтому во многих преступных делах используются преимущественно наличные деньги. Спрос на анонимные платежи привел к разработке систем виртуальной оплаты и виртуальных денег, обеспечивающий анонимные платежи[253]. Виртуальные деньги могут не требовать ни идентификации, ни подтверждения, не давая органам правопорядка отследить денежные потоки в направлении к правонарушителям. В последнее время многие расследования детской порнографии были успешными в обнаружении правонарушителей за счет использования следов, оставленных платежами[254]. Однако там, где правонарушители выполняют анонимные платежи, отследить правонарушителей очень трудно.

2 Использование технологии шифрования[255]

Нарушители все чаще шифруют свои сообщения. Органы правопорядка отмечают, что правонарушители используют технологии шифрования для защиты информации, хранящейся на их жестких дисках[256], это серьезно мешает расследованию преступлений[257].

---

244 *Sieber*, "Council of Europe Organised Crime Report 2004", page 135. Regarding the means of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 et seq., available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

245 See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 5, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

246 See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 5, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

247 For more information, see "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

248 See *Walden*, "Computer Crimes and Digital Investigations", page 66.

249 It is possible to make big profits in a rather short period of time by offering child pornography - this is one way how terrorist cells can finance their activities, without depending on donations.

250 "Police authorities and search engines forms alliance to beat child pornography", available at: http://about.picsearch.com/p_releases/police-authorities-and-search-engines-forms-alliance-to-beat-child-pornography/; "Google accused of profiting from child porn", available at: http://www.theregister.co.uk/2006/05/10/google_sued_for_promoting_illegal_content/print.html.

251 See ABA "International Guide to Combating Cybercrime", page 73.

252 Regarding the use of electronic currencies in money-laundering activities, see: *Ehrlich*, "Harvard Journal of Law & Technology", Volume 11, page 840 et seqq.

253 For more information, see *Wilson*, "Banking on the Net: Extending Bank Regulations to Electronic Money and Beyond".

254 *Smith*, "Child pornography operation occasions scrutiny of millions of credit card transactions",, available at: http://www.heise.de/english/newsticker/news/print/83427.

255 See below: Chapter 3.2.13.

256 Based on the "National Juvenile Online Victimisation Study", 12% of arrested possessors of Internet-related child pornography used encryption technology to prevent access to their files. *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

257 See below: Chapter 3.2.13.

В дополнении к широкому судебному преследованию деяний, связанных с детской порнографией, в настоящее время обсуждаются другие подходы, например, наложение на поставщика услуг доступа в интернет обязательств по регистрации пользователей или по блокировке или фильтрации доступа на веб-сайты, связанные с детской порнографией[258].

2.5.3 Расизм, агрессивные высказывания, восхваление жестокости

Радикальные группы используют средства массовой информации, например интернет для распространения пропагандистских материалов (Рисунок 8[259]). В последнее время увеличилось число веб-сайтов, предлагающих расистский контент и агрессивные высказывания[260], в одном исследовании в 2005 году сделано предположение, что в 2004–2005 годах 25% интернет страниц пропагандируют разжигание национальной розни, насилие и ксенофобию[261]. В 2006 году в интернете существовало более 6000 таких веб-сайтов[262].

Распространение по интернету дает правонарушителям несколько преимуществ, включая малую стоимость распространения, отсутствие специального оборудования и глобальную аудиторию. Среди примеров веб-сайтов, подстрекающих к насилию, находятся веб-сайты, содержащие инструкции по созданию бомб[263]. Помимо пропаганды интернет используется для продажи определенных товаров, например нацистские предметы, таких как флаги с нацистской символикой, униформа и книги свободно доступны на аукционных площадках и специализированных веб-магазинах[264]. Кроме того, интернет используется для отправки электронных писем и новостных рассылок и для распространения видеоклипов и телевизионных программ с использованием популярных архивов, например YouTube.

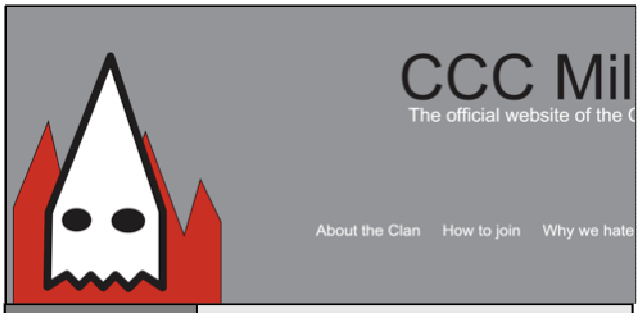


Рисунок 8

На рисунке показан веб-сайт радикальной группы. Интернет интенсивно используется такими группами для сообщения людям о себе и для набора новых членов.

Не во всех странах такие правонарушения преследуются по закону[265]. В некоторых странах такой контент может охраняться принципами свободы слова[266]. Мнения о том, до какой степени к определенным темам применимы принципы свободы слова различны и часто препятствуют международным расследованиям. Одним из примеров конфликта законов является дело 2001 года с участием поставщика услуг Yahoo!, когда французский суд постановил, что компания Yahoo!, расположенная в США, должна блокировать доступ французских пользователей к нацистским материалам[267]. В соответствии с Первой поправкой к Конституции США продажа такого материала законна в соответствии с законами США.

---

258 For an overview about the different obligations of Internet Service Providers that are already implemented or under discussion see: *Gercke*, Obligations of Internet Service Providers with regard to child pornography: legal issue, 2009, available at www.coe.int/cybercrime.

259 Radical groups in the United States recognised the advantages of the Internet for furthering their agenda at an early stage. See *Markoff*, "Some computer conversation is changing human contact", NY-Times, 13.05.1990.

260 *Sieber*, "Council of Europe Organised Crime Report 2004", page 138.

261 *Akdeniz*, "Governance of Hate Speech on the Internet in Europe", in "Governing the Internet Freedom and Regulation in the OSCE Region", page 91, available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

262 See "Digital Terrorism & Hate 2006", available at: http://www.wiesenthal.com.

263 *Whine*, "Online Propaganda and the Commission of Hate Crime", available at: http://www.osce.org/documents/cio/2004/06/3162_en.pdf

264 See "ABA International Guide to Combating Cybercrime", page 53.

265 Regarding the criminalisation in the United States see: *Tsesis*, Prohibiting Incitement on the Internet, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: http://www.vjolt.net/vol7/issue2/v7i2_a05-Tsesis.pdf.

266 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

267 See *Greenberg*, A Return to Liliput: The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market, Berkeley Technology Law Journal, Vol. 18, page 1191 et seq.; *Van Houweling*; Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra, Michigan Journal of International Law, 2003, page 697 et. seq. Development in the Law, The Law of Media, Harvard Law Review, Vol 120, page1041.

В соответствии с Первой поправкой суд США решил, что французское решение для Yahoo! недействительно в Соединенных Штатах Америки.[268]

Различия между странами по этим проблемам было очевидно во время написания проекта Конвенции Совета Европы по киберпреступности. Эта Конвенция старается гармонизировать законы, связанные с киберпреступностью для гарантии того, чтобы конфликты законов не мешали международным расследованиям[269]. Не все стороны, вовлеченные в переговоры, могут согласиться с общей позицией относительно судебного преследования распространения ксенофобных материалов, поэтому эта тема полностью исключена из Конвенции и вместо нее рассмотрена в отдельном Первом протоколе[270]. В ином случае некоторые страны, включая Соединенные Штаты Америки, не смогли бы подписать Конвенцию.

Рисунок 9

На рисунке показан веб-сайт, который предлагает контент с религиозной подоплекой, доступ к которому может быть получен из любой точки мира.

2.5.4 Религиозные преступления

Растущее число[271] веб-сайтов предоставляет материал, который в некоторых странах подпадает под положения, связанные с религиозными преступлениями например письменные антирелигиозные призывы[272]. Хотя некоторые материалы документируют объективные факты и тенденции, например, уменьшение посещений церкви в Европе, эта информация в некоторых юрисдикциях может считаться незаконной. Среди других примеров – диффамация религии или публикация комиксов (Рисунок 9).

Интернет дает преимущества для тех, кто желает обсудить или серьезно работать над некоторым вопросом: люди могут комментировать, передавать материалы или писать статьи, не раскрывая сведений о себе. Множество дискуссионных групп основано на принципе свободы слова[273]. Свобода – это ключевая двигательная сила успеха интернета с порталами, которые используются специально для контента, создаваемого пользователями[274]. Несмотря на то, что защищать этот принцип жизненно важно, даже в наиболее либеральных странах применением принципов свободы слова управляют условия и законы.

Различие законодательных стандартов по запрещенному содержанию отражают проблемы регулирования контента. Даже там, где публикация контента охватывается положениями, касающимися свободы слова, в стране, где этот контент доступен, доступ к этому материалу может быть получен из стран с более строгими законами. "Диспут о комиксах" в 2005 года показал потенциал конфликта. Публикация двенадцати комиксов в датской газете Jyllands-Posten привела к широким протестам в мусульманском мире[275].

---

[268] See“Yahoo Inc. v. La Ligue Contre Le Racisme Et L"antisemitisme”, 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001). Available at: http://www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=213138298941949941944938934938937961519199 1.

[269] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, 144.

[270] See “Explanatory Report to the First Additional Protocol”, No. 4.

[271] See *Barkham*, Religious hatred flourishes on web, The Guardian, 11.05.2004, available at: http://www.guardian.co.uk/religion/Story/0,,1213727,00.html.

[272] Regarding legislative approaches in the United Kingdom see *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.192.

[273] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

[274] *Haraszti*, Preface, in “Governing the Internet Freedom and Regulation in the OSCE Region”, available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

[275] For more information on the “Cartoon Dispute”, see: the Times Online, “70.000 gather for violent Pakistan cartoons protest”, available at: http://www.timesonline.co.uk/tol/news/world/asia/article731005.ece; *Anderson*, “Cartoons of Prophet Met With Outrage”, Washington Post, available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/01/30/AR2006013001316.html; *Rose*, “Why I published those cartoons”, Washington Post, available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/02/17/AR2006021702499.html.

Что касается запрещенного содержания, в раде стран доступность определенной информации или материалов является уголовным преступлением. Защита различных религий или религиозной символики различна в различных странах. В некоторых странах считается преступлением использование агрессивных высказываний в адрес пророка Мохаммеда[276] или осквернение книг священного Корана[277], тогда как в других странах может быть принят более либеральный подход и такие деяния могу не преследоваться по суду.

2.5.5 Незаконные азартные игры и онлайновые игры

Интернет игры и азартные игры – это одна из наиболее быстро растущих областей в интернете[278]. Лаборатория Linden Labs разработчик онлайновой игры Second Life[279] сообщает, что в игре зарегистрировано около десяти миллионов пользователей[280]. Отчеты показывают, что некоторые такие игры используются для совершения преступлений, включая[281]:

Рисунок 10

На рисунке изображен интерфейс пользователя онлайнового казино. После регистрации и перевода денег пользователь может участвовать в онлайновых азартных играх. Многие онлайновые казино позволяют пользоваться услугами без регистрации.

- передачу и воспроизведение детской порнографии[282];
- мошенничество[283];
- азартные игры в[284]; и
- клевета, например, написание оскорбительных или клеветнических сообщений.

По некоторым оценкам прогнозируется рост доходов от онлайновых азартных игр в интернете от 3,1 миллиарда долл. США в 2001 году до 24 миллиардов долл. США в 2010 году[285], хотя по сравнению с доходами от традиционных азартных игр, эти оценки остаются относительно маленькими[286].

В различных странах существует разное регулирование азартных игр в интернете и за пределами интернета[287] – лазейка, которая используется правонарушителями, а также законными предприятиями и казино. Эффект от различного регулирования очевиден в Макао. После того, как макао был возвращен

---

276 Sec. 295-C of the Pakistan Penal Code:
295-C. Use of derogatory remarks, etc., in respect of the Holy Prophet: Whoever by words, either spoken or written, or by visible representation or by any imputation, innuendo, or insinuation, directly or indirectly, defiles the sacred name of the Holy Prophet Mohammed (Peace be Upon Him) shall be punished with death, or imprisonment for life, and shall also be liable to fine.

277 Sec. 295-B of the Pakistan Penal Code:
295-B. Defiling, etc., of Holy Qur'an : Whoever wilfully defiles, damages or desecrates a copy of the Holy Qur'an or of an extract there from or uses it in any derogatory manner or for any unlawful purpose shall be punishable with imprisonment for life.

278 Regarding the growing importance of internet gambling see: *Landes*, "Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation", available at: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Brown/Raysman*, Property Rights in Cyberspace Games and other novel legal issues in virtual property, The Indian Journal of Law and Technology, Vol. 2, 2006, page 87 et seq, available at: http://www.nls.ac.in/students/IJLT/resources/2_Indian_JL&Tech_87.pdf.

279 http://www.secondlife.com.

280 The number of accounts published by Linden Lab. See: http://www.secondlife.com/whatis/. Regarding Second Life in general, see *Harkin*, "Get a (second) life", Financial Times, available at: http://www.ft.com/cms/s/cf9b81c2-753a-11db-aea1-0000779e2340.html.

281 Heise News, 15.11.2006, available at: http://www.heise.de/newsticker/meldung/81088; DIE ZEIT, 04.01.2007, page 19.

282 BBC News, 09.05.2007 Second Life 'child abuse' claim,, available at: http://news.bbc.co.uk/1/hi/technology/6638331.stm.

283 *Leapman*, "Second Life world may be haven for terrorists", Sunday Telegraph, 14.05.2007, available at: http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2007/05/13/nternet13.xml; *Reuters*, "UK panel urges real-life treatment for virtual cash", 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

284 See *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

285 Christiansen Capital Advisor. See http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm.

286 The revenue of United States casinos in 2005 (without Internet gambling) was more than USD 84 billion, from: *Landes*, Layovers And Cargo Ships: "The Prohibition Of Internet Gambling And A Proposed System Of Regulation", page 915, available at: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf;

287 See, for example, GAO, "Internet Gambling - An Overview of the Issues", available at: http://www.gao.gov/new.items/d0389.pdf; Regarding the WTO Proceedings, "US Measures Affecting the Cross-Border Supply of Gambling and Betting Services", see: http://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm; Article 21.5 panel concluded that the United States had failed to comply with the recommendations and rulings of the DSB.

Португалией Китаю в 1999 году, Макао стал одним из самых крупных районов азартных игр в мире. При доходах, оцениваемых в 6,8 миллиардов долл. США в 2006 году, он превзошел Лас Вегас (6,6 миллиардов долл. США)[288]. Успех Макао обусловлен тем, что азартные игры являются незаконными в Китае[289] и тысячи игроков едут играть из континентального Китай в Макао.

Интернет позволяет людям обходить ограничения на азартные игры[290]. Онлайновые казино широко доступны (см. Рисунок 10), большая их часть располагается в странах с либеральными законами или отсутствием законов по азартным играм в интернете. Пользователи могут открыть свой счет в онлайновом режиме, пересылать деньги и играть в азартные игры[291]. Онлайновые казино также могут использоваться для отмывания денег и в действиях по финансированию терроризма[292]. Если правонарушители используют онлайновые казино на этапе пересылки денег, при которой не ведется записей, или они находятся в странах, где отсутствует законодательство против отмывания денег, то органам правопорядка очень трудно определить источники финансирования.

Для стран с ограничениями на азартные игры очень трудно контролировать использование или действия онлайновых казино. Интернет подрывает законодательные ограничения, установленные в некоторых странах на доступ граждан к онлайновым азартным играм[293]. Уже было несколько законодательных попыток воспрепятствовать участию в онлайновых азартных играх[294]: в частности, Закон США "О запрете игорного бизнеса в интернете" 2006 года пытается ограничить незаконные онлайновые азартные игры, наказывая поставщиков финансовых услуг, если они выполняют платежи, связанные с незаконными азартными играми[295].

2.5.6 Клевета и фальшивая информация

Интернет может использоваться для распространения ложной информации также просто как и для обычной информации[296]. Веб-сайты могут содержать фальшивую или клеветническую информацию, особенно на форумах или в комнатах чата, где пользователи могут оставлять сообщения без проверки их модераторами[297]. Молодые люди все чаще используют веб-форумы и социальные сети, где такая

---

[288] For more information, see: BBC News, “Tiny Macau overtakes Las Vegas”, at: http://news.bbc.co.uk/2/hi/business/6083624.stm.

[289] See Art. 300 China Criminal Code:
Whoever, for the purpose of reaping profits, assembles a crew to engage in gambling, opens a gambling house, or makes an occupation of gambling, is to be sentenced to not more than three years of fixed-term imprisonment, criminal detention, or control, in addition to a fine.

[290] Besides gambling in Macau, Chinese have started to use Internet gambling intensively. See: “Online Gambling challenges China's gambling ban”, available at: http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[291] For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

[292] See OSCE Report on Money Laundering Typologies 2000 – 2001, page 3, available at: http://www.oecd.org/dataoecd/29/36/34038090.pdf; *Coates*, Online casinos used to launder cash, available at: http://www.timesonline.co.uk/tol/news/politics/article620834.ece?print=yes&randnum=1187529372681.

[293] See, for example, “Online Gambling challenges China's gambling ban”, available at: http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[294] For an overview of the early United States legislation see: *Olson*, Betting No End to Internet Gambling, Journal of Technology Law and Policy, Vol. 4, Issue 1, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue1/olson.html.

[295] See § 5367 Internet Gambling Prohibition Enforcement Act.

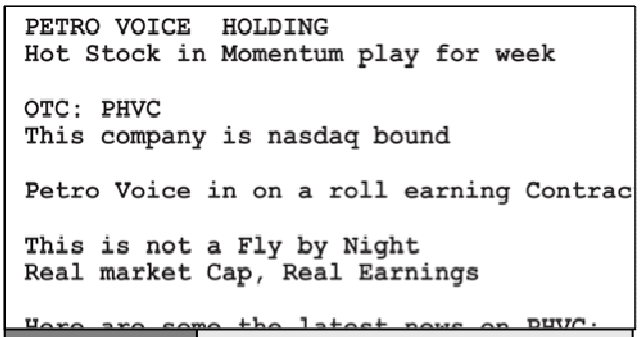
[296] See *Reder/O"Brien*, Corporate Cybersmear: Employers File John Doe Defamation Lawsuits Seeking The Identity Of Anonymous Employee Internet Posters, Mich. Telecomm. Tech. L. Rev. 195, 2002, page 196, available at http://www.mttlr.org/voleight/Reder.pdf.

[297] Regarding the situation in blogs see*: Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington University Law Review, 2006, page 1157 et. seq., available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 et seq., available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol 84, 2006, page 1187 et. seq., available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

информация также может быть размещена[298].

Преступная деятельность[299] может включать в себя, например, публикацию интимных фотографий или ложной информации о сексуальном поведении[300].

В большинстве случаев правонарушители пользуются преимуществами того факта, что поставщики, разрешающие дешевую или бесплатную публикацию, как правило не требуют идентификации авторов или могут не проверять ID[301]. Это усложняет идентификацию правонарушителей. Более того, модераторы форума могут не регулировать или очень мало регулировать контент (Рисунок 11). Эти преимущества не препятствуют разработке ценных проектов, таких как Wikipedia – онлайновая энциклопедия, создаваемая пользователями[302], где существуют строгие процедуры регулирования содержания. Однако правонарушители могут использовать те же самые технологии для:


PETRO VOICE HOLDING
Hot Stock in Momentum play for week

OTC: PHVC
This company is nasdaq bound

Petro Voice in on a roll earning Contrac

This is not a Fly by Night
Real market Cap, Real Earnings

Here are some the latest news on PHVC:

Рисунок 11

Серьезной проблемой являются спамовые электронные письма. Эти электронные письма охватывают широкий диапазон тематик. Кроме рекламы различных продуктов, очень популярно распространение информации о рынках и акциях.

- публикации ложной информации, например о конкурентах[303];
- клеветы, например, оставляя оскорбительные или клеветнические сообщения[304]);
- раскрытия секретной информации, например, публикация государственных секретов или ценной коммерческой информации.

Жизненно важно подчеркнуть растущую опасность, которую представляет собой ложная или вводящая в заблуждение информация. Диффамация может нанести серьезный урон репутации и достоинству жертвы, поскольку онлайновые заявления доступны аудитории по всему миру. В тот момент, когда информация опубликована в интернете, ее автор(ы) часто теряют контроль над этой информацией. Даже если эта информация корректируется или удаляется сразу после публикации, она уже может быть скопирована ("зеркальная копия") и сделана доступной людям, которые не пожелают ее аннулировать или удалить. В таком случае эта информация может оставаться доступной в интернете, даже если она была удалена или исправлена на первоначальном источнике[305]. Примеры включают в себя случаи "электронные письма, отправленные не по тому адресу", в которых миллионы людей могут получить непристойные, вводящие в заблуждение или ложные электронные письма о людях или организациях, когда репутация может никогда не быть восстановлена, вне зависимости от того, является ли это письмо правдой или нет. Следовательно, необходимо сбалансировать свободу слова[306] и защиту потенциальных жертв клеветы[307].

---

[298] Regarding the privacy concerns related to those social networks see: *Hansen/Meissner* (ed.), Linking digital identities, page 8 – An executive summary is available in English (page 8-9). The report is available at: https://www.datenschutzzentrum.de/projekte/verkettung/2007-uld-tud-verkettung-digitaler-identitaeten-bmbf.pdf.

[299] Regarding the controversial discussion about the criminalisation of defamation see: Freedom of Expression, Free Media and Information, Statement of Mr. *McNamara*, US Delegation to the OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf; Regarding the development of the offence see: Walker, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: http://www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: http://www.article19.org/pdfs/standards/definingdefamation.pdf.

[300] See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

[301] With regard to the challenges of investigating offences linked to anonymous services see below: Chapter 3.2.l2.

[302] See: http://www.wikipedia.org

[303] See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

[304] See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

[305] Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as http://www.archive.org

[306] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

2.5.7 Спам и связанные с ним угрозы

"Спам" описывает передачу большого числа незапрашиваемых сообщений (Рисунок 12[308]). Несмотря на то, что существуют различные способы обмана, наиболее широко используемым является спам в электронных письмах. Правонарушители рассылают пользователям миллионы электронных писем, которые часто содержат рекламу продуктов и услуг, но также часто и вредоносные программы. С тех пор, как в 1978 году было отправлено первое спамовое электронное письмо[309], поток спама в электронной почте значительно вырос[310]. Сегодня поставщики услуг электронной почты сообщают, что от 85 до 90% всей электронной почты – спам[311]. В 2007 году основными источниками спама в электронной почте были США (19,6% от общего числа зарегистрированного спама), КНР (8,4%) и Республика Корея (6,5%)[312].

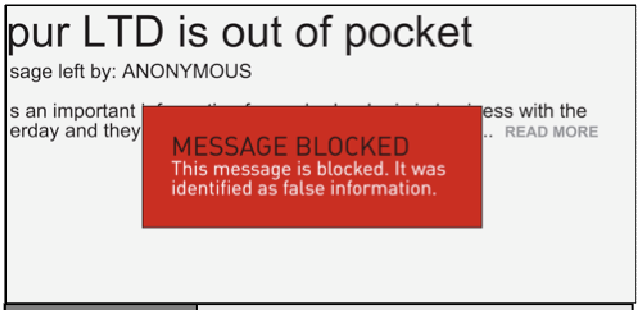


Рисунок 12

Интернет-форумы, где каждый может оставить сообщения без формальной регистрации, это популярные места для того, чтобы оставить сообщение с фальшивой информацией.

Большая часть поставщиков услуг электронной почты реагируют на растущие уровни спама в электронной почте путем установки антиспамовых технологий. Эти технологии идентифицируют спам при помощи фильтрации по ключевым словам или ведения черных списков IP-адресов спаммеров[313]. Несмотря на то, что технология фильтрации продолжает развиваться, спаммеры находят пути обхода этих систем, например, избегая использовать ключевые слова. Спаммеры нашли множество способов написания слова "Виагра" – одного из наиболее популярных продуктов, предлагаемых в спаме, без использования названия бренда[314].

Успех в обнаружении спама в электронной почте зависит от изменений способов распространения спама. Вместо передачи сообщений с одного почтового сервера, что технически легче определяется поставщиками услуг электронной почты из-за ограниченного числа источников[315], многие правонарушители для распространения незапрошенных электронных писем пользуются сетевыми роботами[316]. При использовании сетевых роботов, созданных из тысяч компьютерных систем[317], каждый компьютер может передавать только несколько сотен электронных писем. Это усложняет работу поставщиков услуг электронной почты по

---

307 See in this context: *Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington University Law Review, 2006, page 1157 et. seq., available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 et seq., available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol 84, 2006, page 1187 et. seq., available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

308 For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

309 *Tempelton*, "Reaction to the DEC Spam of 1978", available at: http://www.templetons.com/brad/spamreact.html.

310 Regarding the development of spam e-mails, see: *Sunner*, 'security Landscape Update 2007", page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

311 The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails were spam. See: http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf. The provider Postini published a report in 2007 identifying up to 75 per cent spam e-mail, see http://www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mail, see http://spam-filter-review.toptenreviews.com/spam-statistics.html.
Article in The Sydney Morning Herald, "2006: The year we were spammed a lot", 16 December 2006; http://www.smh.com.au/news/security/2006-the-year-we-were-spammed-a-lot/2006/12/18/1166290467781.html, available April 2007.

312 "2007 Sophos Report on Spam-relaying countries", available at: http://www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

313 For more information about the technology used to identify spam e-mails see *Hernan/Cutler/Harris*, Email Spamming Countermeasures: Detection and Prevention of Email Spamming, available at: http://www.ciac.org/ciac/bulletins/i-005c.shtml; For an overview on different approaches see: BIAC ICC Discussion Paper on SPAM, 2004, available at: http://www.itu.int/osg/csd/spam/contributions/ITU%20workshop%20on%20spam%20BIAC%20ICCP%20Spam%20Discussion%20Paper.pdf

314 Lui/Stamm, "Fighting Unicode-Obfuscated Spam", 2007, page 1, available at: http://www.ecrimeresearch.org/2007/proceedings/p45_liu.pdf.

315 Re the filter technologies available, see: Goodman, 'spam: Technologies and Politics, 2003", available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam, "Consumer Perspectives On Spam: Challenges And Challenges", available at: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

316 Botnets is a short term for a group of compromised computers running programmes that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: http://www.fas.org/sgp/crs/terror/RL32114.pdf.

317 Current analyses suggest that up to a quarter of all computer systems may have been recruited to act as part of botnets. See *Weber*, "Criminals may overwhelm the web", BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

идентификации спама путем анализа информации об отправителях и усложняет органам правопорядка задачу по отслеживанию правонарушителей.

Спамовые электронные письма чрезвычайно прибыльны, так как стоимость рассылки миллиардов электронных писем очень низка и еще ниже, если используются сетевые роботы[318]. Некоторые эксперты предполагают, что единственным реальным решением по борьбе со спамом является повышение стоимости передачи для отправителя[319]. В отчете, опубликованном в 2007 году, проанализированы затраты и доходы от спама в электронной почте. На основе результатов этого анализа, стоимость рассылки 20 миллионов электронных писем составляет примерно 500 долл. США[320]. Поскольку расходы для правонарушителей малы, то рассылка спама является очень прибыльной, особенно, если правонарушители смогут разослать миллиарды электронных писем. Датский спаммер сообщает о получении прибыли примерно 50 000 долл. США за рассылку примерно 9 миллиардов спамовых электронных писем[321].

В 2005 году ОЭСР опубликовал отчет, анализирующий влияние спама на развивающиеся страны[322]. Развивающиеся страны часто высказывают мысль, что пользователи интернета в их странах больше страдают от спама и неправомерного использования интернета. Спам – это серьезная проблема в развивающихся странах, где полоса пропускания канала доступа в интернет дефицитна и стоит дороже, чем в промышленно развитых странах[323]. Спам использует ценные ресурсы и время в странах, где ресурсы интернет более ограниченны и стоят дороже.

2.5.8 Другие формы незаконного контента

Интернет используется не только для прямых атак, но также и как форум для:

- подстрекательства, предложений и побуждения к совершению преступлений[324];
- незаконной продажи продуктов; и
- предоставления информации и инструкции для незаконных действий, например, как сделать взрывчатку.

Во многих странах приняты законы по торговле определенными продуктами. В различных странах применяются различные национальные законы и ограничения по торговле различными продуктами, например военным оборудованием[325]. Аналогичная ситуация существует для лекарств: лекарства, которые продаются без ограничений в некоторых странах, в других могут отпускаться только по рецептам[326]. Трансграничная торговля может затруднить гарантировать такое положение дел, при котором на определенной территории ограничен доступ к определенным продуктам[327]. Учитывая популярность интернета, эта проблема растет. Веб-магазины, работающие в странах без ограничений, могут продавать продукты потребителям в других странах, где действуют запреты, подрывая эти ограничения.

---

318 Regarding inernational approaches in the fight against Botnets see: ITU Botnet Mitigation Toolkit, Background Information, ICT Application and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Sector, 2008, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-botnet-mitigation-toolkit-background.pdf.

319 See: *Allmann*, "The Economics of Spam", available at: http://acmqueue.org/modules.php?name=Content&pa=showpage&pid=108; *Prince*, ITU Discussion Paper "Countering Spam: How to Craft an Effective Anti-Spam Law", page 3 with further references, available at: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_How%20to%20craft%20and%20effective%20anti-spam%20law.pdf.

320 Bulk discounts for spam, Heise News, 23.10.2007, available at: http://www.heise-security.co.uk/news/97803.

321 *Thorhallsson*, "A User Perspective on Spam and Phishing", in "Governing the Internet Freedom and Regulation in the OSCE Region", page 208, available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf

322 'spam Issue in Developing Countries", available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

323 See 'spam Issue in Developing Countries", Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

324 See *Sieber*, Council of Europe Organised Crime Report 2004, page 140.

325 See for example the United States International Traffic in Arms Regulation or the Wassenaar Agreement, which is a convention on arms control. 40 countries already participate in the agreement. For more information, see: http://www.wassenaar.org/publicdocuments/whatis.html or *Grimmett*, Military Technology and Conventional Weapons Export Controls: The Wassenaar Arrangement.

326 See in this context: Council of Europe, Resolution ResAP(2007)2 on good practices for distributing medicines via mail order which protect patient safety and the quality of the delivered medicine, available at: https://wcd.coe.int/ViewDoc.jsp?Ref=ResAP(2007)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75.

327 See for example *Henney*, "Cyberpharmacies and the role of the US Food And Drug Administration", available at: https://tspace.library.utoronto.ca/html/1807/4602/jmir.html; *De Clippele*, Legal aspects of online pharmacies, Acta Chir Belg, 2004, 104, page 364, available at: http://www.belsurg.org/imgupload/RBSS/DeClippele_0404.pdf; *Basal*, "What's a Legal System to Do? The Problem of Regulating Internet Pharmacies", available at: https://www.tnybf.org/success%20stories/2006%20Meyer%20Scholarship%20Recipient%20Essay.pdf.

До появления интернета большинству людей было сложно получить инструкции по созданию оружия. Необходимая информация была доступна например в книгах, рассматривающих химию взрывчатых веществ, но для того чтобы ее найти, требовалось время. Сегодня информация о том, как сделать взрывчатку доступна в интернете[328], и простота доступа к этой информации повышает вероятность атак.

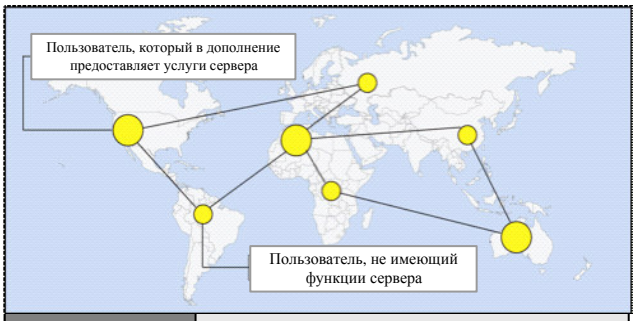


Рисунок 13

На рисунке показана работа систем обмена файлами второго поколения. Системы обмена файлами первого поколения работали с централизованными серверами, на которых лежал список доступных документов. В системах обмена файлами второго поколения. Функции сервера делегированы пользователям, что затрудняет нарушение работы сети и предотвращает нарушение авторских прав.

2.6 Преступления, связанные с правами собственности и товарными знаками

Одной из главнейших функций интернета является распространение информации. Компании используют интернет для распространения информации о своих продуктах и услугах. Если говорить о пиратстве, успешные компании могут столкнуться в интернете с проблемами, сравнимыми с теми, которые существуют вне сети. Престиж их марки и фирменный дизайн могут использоваться для сбыта поддельных продуктов, когда производители контрафакта копируют как логотипы, так и сами продукты и пытаются зарегистрировать домен, связанный с этой определенной компанией. Компании, распространяющие продукцию напрямую через интернет[329], могут столкнуться с правовыми проблемами, связанными с нарушениями авторских прав. Их продукция может быть загружена, скопирована и распространена.

2.6.1 Преступления, связанные с авторскими правами

С переходом с аналоговых форматов на цифровые[330], оцифровка[331] позволила индустрии развлечений добавлять к фильмам на DVD дополнительные функции и услуги, включая языки, субтитры, трейлеры и бонусный материал. Компакт-диски и DVD-диски доказали большую жизнеспособность, чем аудио- и видеокассеты[332].

Оцифровка открыла новый способ нарушений авторских прав. Основой существующих нарушений авторских прав является быстрое и точное воспроизведение. До оцифровки копирование аудио- и видеокассет всегда приводило к некоторому снижению качества. В настоящее время можно скопировать цифровой источник без потери качества, а также, в результате, делать копии с любой копии. Наиболее часто встречающиеся нарушения авторских прав включают в себя:

- Обмен в файлообменных сетях песнями, файлами и программным обеспечением, защищаемыми авторским правом[333];
- Обход систем технологии управления цифровыми правами[334];

Файлообменные системы являются сетевыми услугами на основе одноранговых[335] отношений, которые позволяют пользователям пользоваться файлами совместно[336], часто с миллионами других пользователей[337].

---

328 See: See *Conway*, "Terrorist Uses of the Internet and Fighting Back, Information and Security", 2006, page 16, United States Department of Justice 1997 Report on the availability of bomb-making information, available at: http://www.usdoj.gov/criminal/cybercrime/bombmakinginfo.html; *Sieber*, Council of Europe Organised Crime Report 2004, page 141.

329 E.g. by offering the download of files containing music, movies or books.

330 Regarding the ongoing transition process, see: "OECD Information Technology Outlook 2006", Highlights, page 10, available at: http://www.oecd.org/dataoecd/27/59/37487604.pdf.

331 See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, Page 34 et seqq.

332 Besides these improvements, digitalisation has speeded up the production of the copies and lowered the costs that were one of the key drivers for the industry to perform the transition to digital-based technologies.

333 *Sieber*, Council of Europe "Organised Crime Report 2004", page 148.

334 Digital Rights Management describes access control technology used to limit the usage of digital media. For further information, see: *Cunard/Hill/Barlas*, "Current developments in the field of digital rights management", available at: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf. Baesler, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: http://www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf.

335 Peer-to-Peer (P2P) describes direct connectivity between participants in networks instead of communicating over conventional centralized server-based structures. See: *Schoder/Fischbach/Schmitt*, "Core Concepts in Peer-to-Peer Networking, 2005", available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, "A Survey of Peer-to-Peer Content Distribution Technologies, 2004", available at: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

После установки программ для обмена файлами, пользователи могут выбрать файлы для совместного использования и использовать программу для поиска файлов, предлагаемый в сети другими пользователями, для скачивания с сотен источников. До разработки файлообменных систем люди копировали записи и пленки и обменивались ими, но файлообменные системы дают возможность обмениваться копиями гораздо большему числу пользователей.

Технология одноранговых (P2P) взаимоотношений играет в интернете важную роль. В настоящее время более 50% потребительского интернет-трафика создается одноранговыми сетями[338]. Число пользователей постоянно растет, в отчете, опубликованном ОЭСР, утверждается, что примерно 30% пользователей интернета во Франции загружали музыку или файлы в файлообменных системах[339], другие страны ОЭСР демонстрируют те же тенденции[340]. Файлообменные системы можно использовать для обмена компьютерными данными любого вида, включая музыку, фильмы и программное обеспечение[341]. Исторически файлообменные системы использовались преимущественно для обмена музыкой, но обмен видеофайлами становится все более значительным[342].

Технология, используемая в файлообменных услугах, очень сложная и позволяет обмениваться большими файлами за короткий период времени[343]. Файлообменные системы первого поколения зависели от центрального сервера, позволяя органам охраны правопорядка действовать против незаконного файлообмена в сети Napster[344]. В отличие от систем первого поколения (особенно, известной службы Napster), файлообменные системы второго поколения более не основываются на центральном сервере, представляющем список доступных пользователям файлов[345]. Концепция децентрализации файлообменных сетей второго поколения (см. Рисунок 13) намного усложнила предотвращение их работы. Однако благодаря прямой связи можно отслеживать пользователей сети по их IP-адресам[346]. Органы охраны правопорядка достаточно успешно расследовали нарушения авторских прав в файлообменных системах. Более новые версии файлообменных систем позволяют создавать анонимные связи и еще более усложняют расследования[347].

---

336 GAO, File Sharing, "Selected Universities Report Taking Action to Reduce Copyright Infringement", available at: http://www.gao.gov/new.items/d04503.pdf; *Ripeanu/Foster/Iamnitchi*, Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design, available at: http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf. United States Federal Trade Commission, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, page 3, available at: http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems, available at: http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

337 In 2005, 1.8 million users used Gnutella. See *Mennecke*, "eDonkey2000 Nearly Double the Size of FastTrack", available at: http://www.slyck.com/news.php?story=814.

338 See Cisco" Global IP Traffic Forecast and Methodology", 2006-2011, 2007, page 4, available at: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns537/c654/cdccont_0900aecd806a81aa.pdf.

339 See: "OECD Information Technology Outlook 2004", page 192, available at: http://www.oecd.org/dataoecd/22/18/37620123.pdf.

340 One example is Germany, where a regularly updated report of the Federation of the phonographic businesses pointed out that, in 2006, 5.1 million users in Germany downloaded music in file-sharing systems. The report is available at: http://www.ifpi.de/wirtschaft/brennerstudie2007.pdf. Regarding the United States see: *Johnson/McGuire/Willey*, "Why File-Sharing Networks Are Dangerous", 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

341 Apart from music, videos and software, even sensitive personal documents are often found in file-sharing systems. See: *Johnson/McGuire/Willey*, "Why File-Sharing Networks Are Dangerous", 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf.

342 While in 2002, music files made up more than 60% of all files exchanged in file-sharing systems in OECD countries, this proportion dropped in 2003 to less than 50%. See: "OECD Information Technology Outlook 2004", page 192, available at: http://www.oecd.org/dataoecd/22/18/37620123.pdf.

343 *Schoder/Fischbach/Schmitt*, "Core Concepts in Peer-to-Peer Networking", 2005, page 11, available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Cope, Peer-to-Peer Network, Computerworld, 8.4.2002, available at: http://www.computerworld.com/networkingtopics/networking/story/0,10801,69883,00.html; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

344 Regarding Napster and the legal response see: *Rayburn,* After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: http://www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html. *Penn*, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol7/issue2/penn.pdf.

345 Regarding the underlying technology see: *Fischer*, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002, available at: http://www.vjolt.net/vol7/issue3/v7i3_a07-Fisher.pdf; *Sifferd*, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: http://www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; Herndon, Who's watching the kids? – The use of peer-to-peer programs to Cyberstalk children, Oklahoma Journal of Law and Technology, Vol. 12, 2004, available at: http://www.okjolt.org/pdf/2004okjoltrev12.pdf; *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

346 For more information on investigations in peer-to-peer networks, see: "Investigations Involving the Internet and Computer Networks", NIJ Special Report, 2007, page 49 et seqq., available at: http://www.ncjrs.gov/pdffiles1/nij/210798.pdf.

347 *Clarke/Sandberg/Wiley/Hong*, "Freenet: a distributed anonymous information storage and retrieval system", 2001;

Файлообменная технология используется не только обычными людьми и преступниками, но и обычными компаниями[348]. Не все файлы в файлообменных системах нарушают авторские права. Примеры их правомерного использования включают обмен законными копиями или иллюстрациями на некоммерческой основе[349].

Тем не менее, использование файлообменных систем бросает вызов индустрии развлечений[350]. Непонятно, до какого уровня снизятся продажи CD/DVD-дисков и билетов в кинотеатры из-за обмена фильмами в файлообменных сетях. В результате исследования были выявлены миллионы пользователей файлообменных сетей[351] и миллиарды загруженных файлов[352]. Копии фильмов появляются в файлообменных сетях раньше их официального проката в кинотеатрах[353], что отражается на доходах правообладателей. Недавнее появление анонимных файлообменных систем еще более затрудняет работу как правообладателей, так и органов охраны правопорядка[354].

Индустрия развлечений ответила внедрением технологии, предназначенной для предотвращения изготовления пользователями копий CD и DVD-дисков, например, Систем шифрования содержания (CSS[355]), в которой технология шифрования мешает копированию содержимого DVD-дисков[356]. Эта технология является важным элементом новых бизнес-моделей, предназначенных для более четкого распределения прав доступа пользователям. Управление цифровыми правами (DRM[357]) описывает внедрение технологий, позволяющих правообладателям запрещать использование цифровых носителей, когда пользователи покупают только ограниченные права, например право воспроизведения песни на одной вечеринке. DRM предлагает возможность внедрения новых бизнес-моделей, более точно отражающих интересы правообладателей и пользователей и позволяющих уменьшить снижение прибыли.

Одной из главных проблем данных технологий является то, что технологии защиты авторских прав можно обойти[358]. Злоумышленники разработали программные инструменты, позволяющие пользователям делать файлы с защитой от копирования доступными в интернете[359] бесплатно или по небольшой стоимости. Как только с файла снята защита DRM, его можно копировать и воспроизводить без ограничений.

Попытки защитить содержимое не ограничивается песнями и фильмами. Некоторые телестанции, особенно платные телеканалы, шифруют программы для гарантии того, что программу смогут получать только абоненты, заплатившие за это. Хотя технологии защиты очень сложны, злоумышленники успешно подделывают аппаратные средства, используемые для получения контроля или взлома шифрования при помощи программных инструментов[360].

Маловероятно, что обычные пользователи смогут совершать преступления, не имея программных инструментов. Обсуждения судебного преследования нарушения авторских прав сосредотачивается не

Chothia/Chatzikokolakis, "A Survey of Anonymous Peer-to-Peer File-Sharing", available at: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Desing", 2005.

348 Regarding the motivation of users of peer-to-peer technology see: *Belzley*, Grokster and Efficiency in Music, Virginia Journal of Law and Technology, Vol. 10, Issue 10, 2005, available at: http://www.vjolt.net/vol10/issue4/v10i4_a10-Belzley.pdf.

349 For more examples, see: Supreme Court of the United States, Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd, I. B., available at: http://fairuse.stanford.edu/MGM_v_Grokster.pdf.

350 Regarding the economic impact, see: *Liebowitz*, "File-Sharing: Creative Destruction or Just Plain Destruction", Journal of Law and Economics, 2006, Volume 49, page 1 et seqq.

351 The latest analysis regarding file-sharing activities in Germany identify up to 7.3 million users who download music files from the Internet. Up to 80% of these downloads are related to file-sharing systems. Source: GfK, Brennerstudie 2005.

352 "The Recording Industry 2006 Privacy Report", page 4, available at: http://www.ifpi.org/content/library/piracy-report2006.pdf.

353 One example is the movie, "Star Wars – Episode 3", that appeared in file-sharing systems hours before the official premiere. See: http://www.heise.de/newsticker/meldung/59762 that is taking regard to a MPAA press release.

354 Regarding anonymous file-sharing systems, see: *Wiley/ Hong*, "Freenet: A distributed anonymous information storage and retrieval system", in Proceedings of the ICSI Workshop on Design Issues in Anonymity and Unobservability, 2000.

355 Content Scrambling Systems (CSS) is a Digital Rights Management system that is used is most DVD videos discs. For details about the encryption used, see *Stevenson*, "Cryptanalysis of Contents Scrambling System", available at: http://www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm.

356 Regarding further responses of the entertainment industry (especially lawsuits against Internet user) see: *Fitch*, From Napster to Kazaa: What the Recording Industry did wrong and what options are left, Journal of Technology Law and Policy, Vol. 9, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol9/issue2/fitch.html.

357 Digital Rights Management describes access control technology used to limit the usage of digital media. For more information, see: *Cunard/Hill/Barlas*, "Current developments in the field of digital rights management", available at: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, "Digital Rights Management: The Skeptics' View", available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

358 *Bloom/Cox/Kalker/Linnartz/Miller/Traw*, "Copy Protection for DVD Videos"", IV 2, available at: http://www.adastral.ucl.ac.uk/~icox/papers/1999/ProcIEEE1999b.pdf

359 *Sieber*, Council of Europe Organised Crime Report 2004, page 152.

360 See: http://www.golem.de/0112/17243.html.

только на файлообменных сетях и обходе технической защиты, но и на создании, продаже и обладании "нелегальными устройствами" или инструментами предназначенными для предоставления пользователям возможности совершать нарушения авторских прав[361].

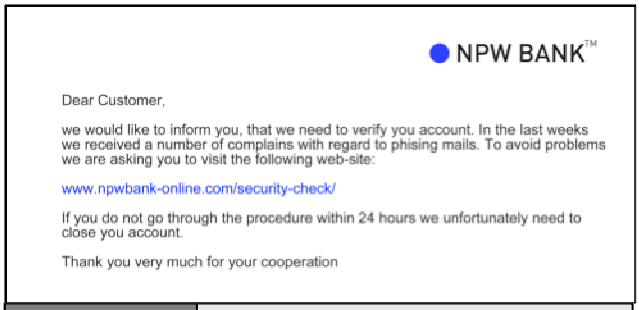
2.6.2 Преступления, связанные с товарными знаками

Преступления, связанные с товарными знаками, похожи на нарушения авторских прав – хорошо известный аспект международной торговли. Преступления, связанные с товарными знаками, перешли в киберпространство, и в уголовном праве разных стран они преследуются по закону до различной степени[362]. Наиболее тяжкие преступления включают в себя:

- Использование товарных знаков в совершении преступлений с целью введения жертвы в заблуждение; и
- Преступления, связанные с доменами или именами.

Доброе имя компании часто напрямую связано с ее товарными знаками. Злоумышленники используют фирменные и товарные знаки обманным путем для некоторых действий, включая фишинг (см. Рисунок 14[363]), когда миллионы электронных писем отправляются пользователям интернета, аналогичных электронным письмам от законных компаний, например, включая товарные знаки[364].

Другим вопросом, относящимся к преступлениям, с товарными знаками, являются преступления, связанные с доменами[365], например киберсквоттинг[366], который представляет собой процесс незаконной регистрации доменных имен, идентичных или похожих на товарные знаки продукции или компании[367]. В большинстве случаев злоумышленник стремится продать домен по высокой цене компании[368] или использовать его для продажи продукции или услуг, вводя пользователей в заблуждение при помощи их предполагаемого отношения к данному товарному знаку[369].


NPW BANK™

Dear Customer,

we would like to inform you, that we need to verify you account. In the last weeks we received a number of complains with regard to phising mails. To avoid problems we are asking you to visit the following web-site:

www.npwbank-online.com/security-check/

If you do not go through the procedure within 24 hours we unfortunately need to close you account.

Thank you very much for your cooperation

Рисунок 14

На рисунке показано фишинг-сообщение. Фишинг-сообщения предназначены для имитации сообщений от законных компаний. Правонарушители часто используют оригинальные логотипы, охраняемые законами о товарных знаках.

361 Regarding the similar discussion with regard to tools used to design viruses, see below: Chapter 2.7.4.

362 See Bakken, Unauthorised use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Regarding trademark violations as a consequence of online-criticism see: *Prince*, Cyber-Criticism and the Federal Trademark Dilution act: Redefining the Noncommercial use Exemption, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: http://www.vjolt.net/vol9/issue4/v9i4_a12-Prince.pdf;

363 The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, The criminalisation of Phishing and Identity Theft, Computer und Recht, 2005, 606; *Ollmann*, "The Phishing Guide: Understanding & Preventing Phishing Attacks", available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: Chapter 2.8.d.

364 For an overview about what phishing mails and the related spoofing websites look like, see: http://www.antiphishing.org/phishing_archive/phishing_archive.html

365 Re the connection with trademark-related offences, see for example: "Explanatory Report to the Convention on Cybercrime", No. 42.

366 Another term used to describe the phenomenon is "domain grabbing". Regarding cyber-squatting see: *Hansen-Young*, Whose Name is it, Anyway? Protecting Tribal Names from Cybersquatters, Virginia Journal of Law and Technology, Vol. 10, Issue 6; *Benoliel*, Cyberspace Technological Standandization: An Institutional Theory Retrospective, Berkeley Technology Law Journal, Vol. 18, page 1259 et seq.; *Struve/Wagner*, Realspace Sovereignty in Cyberspace: Problems with the Anticybersquatting Consumer Protection Act, Berkeley Technology Law Journal, Vol. 17, page 988 et seq.; *Travis*, The Battle for Mindshare: The Emerging Consesus that the First Amendment Protects Corporate Criticism and Parody on the Internet, Virginia Journal of Law and Technology, Vol. 10, Issue 3, 2003;

367 See: *Lipton*, "Beyond cybersquatting: taking domain name disputes past trademark policy", 2005, available at: http://www.law.wfu.edu/prebuilt/w08-lipton.pdf.

368 This happens especially with the introduction of new top-level-domains. To avoid cyber-squatting, the introduction of a new first-level domain is often accompanied by a period where only parties with trademarks can register a domain name. At the end of this phase (often called the "sunrise period"), other users can register their domain.

369 For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 112.

Другим примером преступления, связанного с доменом, является "угон домена" или регистрация доменных имен, которые были случайно утеряны.[370]

2.7 *Преступления, связанные с компьютерами*

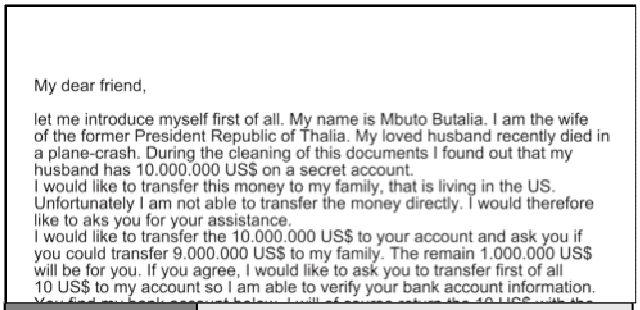
В эту категорию входят некоторые преступления, для совершения которых требуется компьютерная система. В отличие от предыдущих категорий защита от этого широкого класса преступления, определяемая правовыми принципами, зачастую не так строга, включая в себя:

- мошенничество с использованием компьютера;
- подлог с использованием компьютера, фишинг и кражу идентичности; и
- неправильное использование устройств.

2.7.1 Мошенничество и компьютерное мошенничество

Мошенничество с использованием компьютера – одно из самых популярных преступлений в интернете[371], так как позволяет преступнику применять для сокрытия своей личной информации автоматизацию[372] и программные инструменты.

Автоматизация позволяет злоумышленникам получать большие преимущества при условии выполнения нескольких небольших действий[373]. Одной из стратегий, используемых злоумышленниками, является уверенность в том, что финансовые потери каждой жертвы ниже определенного уровня. При "небольших" потерях жертва с меньшей вероятностью будет тратить время и энергию для сообщения и расследования таких преступлений[374]. Одним из примеров такой аферы является Нигерийское мошенничество с предоплатой (см. Рисунок 15[375]).


My dear friend,

let me introduce myself first of all. My name is Mbuto Butalia. I am the wife of the former President Republic of Thalia. My loved husband recently died in a plane-crash. During the cleaning of this documents I found out that my husband has 10.000.000 US$ on a secret account.
I would like to transfer this money to my family, that is living in the US. Unfortunately I am not able to transfer the money directly. I would therefore like to aks you for your assistance.
I would like to transfer the 10.000.000 US$ to your account and ask you if you could transfer 9.000.000 US$ to my family. The remain 1.000.000 US$ will be for you. If you agree, I would like to ask you to transfer first of all 10 US$ to my account so I am able to verify your bank account information.

Рисунок 15

На графике показано классическое электронное письмо на основе расширенной аферы с мошенничеством с вознаграждением. Для получения предполагаемой прибыли, адресату требовалось перевести авансом определенную сумму. Это очень популярное мошенничество, но так как оно не использует махинации с компьютерными системами, оно не является аферой, связанной с компьютером.

Хотя эти преступления совершаются при помощи компьютерных технологий, большинство систем уголовного права рассматривают их не как преступления, связанные с компьютерами, а как обычное мошенничество[376]. Основным различием между мошенничеством, связанным с компьютером и обычным мошенничеством является жертва мошенничества. Если злоумышленники пытаются повлиять на человека, преступление обычно классифицируется как мошенничество. Если целью злоумышленника являются компьютерные системы или системы по обработке данных, то преступления зачастую классифицируются как мошенничество с использованием компьютера. Те системы уголовного права, которые описывают мошенничество, но пока не включают в себя махинации с компьютерными системами в мошеннических целях, зачастую все-таки могут преследовать упомянутые преступления.

---

370 For case examples, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 113.

371 In 2006, the United States Federal Trade Commission received nearly 205,000 Internet-related fraud complaints. See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

372 Regarding the related challenges see below: Chapter 3.2.8.

373 In 2006, Nearly 50% of all fraud complaints reported to the United States Federal Trade Commission were related to amounts paid between 0-25 US Dollars See Consumer Fraud and Identity Theft Complaint Data, January – December 2006, Federal Trade Commission, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

374 Regarding the related automation process: Chapter 3.2.8.

375 The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, "Trends & Issues in Crime and Criminal Justice", No. 121, available at: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, "Advance fee fraud on the Internet: Nigeria's regulatory response", "Computer Law & Security Report", Volume 21, Issue 3, 237.

376 For more information, see below: Chapter 6.1.13.

К наиболее распространенным мошенническим аферам относятся:

1 Мошенничество с онлайновыми аукционами[377]

Онлайновые аукционы в настоящее время являются одними из самых популярных услуг электронной коммерции. В 2006 году через eBay, самую большую в мире онлайновую аукционную площадку, было продано товаров на сумму более 20 млрд. долл. США[378]. Покупатели могут получить доступ к разным товарам или товарам определенной категории из любой точки мира. Продавцы получают предложения со всего мира, стимулируя спрос и повышение цен.

Злоумышленники, совершающие преступления на аукционных площадках, могут использовать отсутствие личного контакта между продавцом и покупателем[379]. Трудность, связанная с нахождением отличия между настоящим пользователем и злоумышленником, привела к тому, что мошенничество с аукционом стало одним из самых популярных видов киберпреступлений[380]. Два самых распространенных вида афер включают в себя[381]:

- Выставление на продажу несуществующих товаров и требование авансовой оплаты покупки до ее доставки[382]; или
- Покупка товаров и просьба доставить без намерения оплатить.

В ответ поставщики услуг аукциона разработали системы защиты, например систему отзывов/комментариев. После каждой сделки покупатели и продавцы оставляют отзывы для других пользователей[383] в качестве нейтральной информации о надежности продавца/покупателя. В таком случае "репутация – это все", и без достаточного количества положительных комментариев злоумышленникам трудно принудить жертвы либо к оплате несуществующих товаров, либо, наоборот, к отправке товара без предварительной его оплаты.

Однако преступники в ответ обошли эту защиту при помощи регистрации от имени третьего лица[384]. В такой афере, называемой "захват счета"[385], злоумышленники пытаются завладеть именами пользователя и паролями законных пользователей для покупки или продажи мошенническим образом, что усложняет идентификацию злоумышленников.

2 Мошенничество с предоплатой[386]

В мошенничестве с предоплатой злоумышленники отправляют электронные письма адресату с просьбой о помощи в переводе больших сумм денег третьим лицам и обещанием им процента, если он согласится произвести перевод через свой личный счет[387]. Затем злоумышленники просят его перевести небольшую

---

377 The term auction fraud describes fraudulent activities involving electronic auction platforms over the Internet. Regarding auction fraud see: *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 et seq., available at: http://www.aslib.co.uk/proceedings/protected/2001/jul-aug/03.pdf; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 et seq.; *Chau/Faloutsos*, Fraud Detection in Electronic Auction, available at: http://www.cs.cmu.edu/~dchau/papers/chau_fraud_detection.pdf; Dolan, Internet Auction Fraud: The Silent Victims, Journal of Economic Crime Management, Vol. 2, Issue 1, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/BA2DF0D2-D6ED-10C7-9CCB88D5834EC498.pdf.

378 See http://www.ebay.com.

379 See *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1;

380 The United States Internet Crime Complaint Centre (IC3) (a partnership between the FBI and the National White Collar Crime Centre) reported that around 45% of complaints refer to Auction Fraud. See: "IC3 Internet Crime Report 2006", available at: http://www.ic3.gov/media/annualreport/2006_IC3Report.pdf

381 "Law Enforcement Efforts to combat Internet Auction Fraud", Federal Trade Commission, 2000, page 1, available at: http://www.ftc.gov/bcp/reports/int-auction.pdf.

382 See: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

383 For more information, see for example: http://pages.ebay.com/help/feedback/feedback.html.

384 Regarding the criminalisation of "account takeovers", see *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

385 See "Putting an End to Account-Hijacking Identity Theft", Federal Deposit Insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

386 The term "advance fee fraud" describes offences in which offenders seek to convince targets to advance a small sum of money in the hope of receiving a much larger sum afterwards. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1. For more information, see: *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1, page 1; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, "Trends & Issues in Crime and Criminal Justice", No. 121, available at: http://www.aic.gov.au/publications/tandi/ti121.pdf; *Oriola*, "Advance fee fraud on the Internet: Nigeria's regulatory response", "Computer Law & Security Report", Volume 21, Issue 3, 237; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7, available at: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

387 Advance Fee Fraud, Foreign & Commonwealth Office, available at: http://www.fco.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1044901630595.

сумму денег для подтверждения данных о его банковском счете, здесь основа – поведение, аналогичное лотереям: респонденты могут пожелать понести небольшие, но определенные, затраты в обмен на большую, но неопределенную, выгоду; или просто просят выслать данные о банковом счете. Как только жертва переведет деньги, она больше никогда снова не услышит о злоумышленнике. Если будет передана информация о банковском счете, злоумышленники могут использовать эту информацию для мошеннической деятельности. Доказательства показывают, что тысячи жертв отвечали на электронные сообщения[388]. Исследования, проводимые в настоящее время, показали, что, несмотря на различные информационные кампании и инициативы, число мошенничеств с предоплатой продолжает расти как по количеству жертв, так и по общим потерям[389].

2.7.2 Подлог с использованием компьютера

Подлог с использованием компьютера описывает махинации с цифровыми документами[390], например:

- создание документа, который, как кажется, происходит от надежной организации;
- подделка электронных изображений, например изображений, используемых в качестве доказательств в суде; или
- изменение текстовых документов.

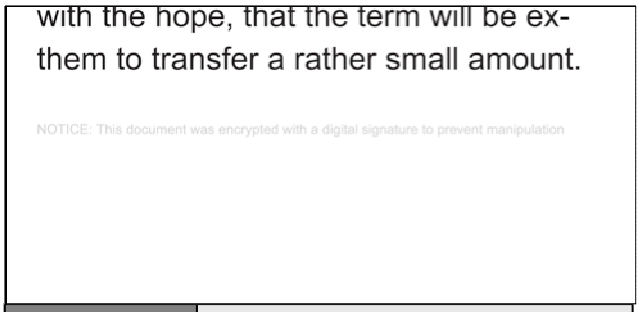


Рисунок 16

В сравнении с фальсификацией обычного документа электронные данные подделать гораздо проще. Такие технические решения, как цифровая подпись, могут предотвратить непризнанные махинации.

Фальсификация электронных писем включает аферу "фишинг", являющуюся сложной проблемой для органов охраны правопорядка по всему миру[391]. "Фишинг" стремится заставить свою жертву раскрыть личную/секретную информацию[392]. Зачастую злоумышленники отправляют электронные сообщения, которые выглядят, как сообщения от законных финансовых учреждений, используемых жертвой[393]. Электронные письма создаются так, что жертве трудно определить, что это ложное электронное сообщение[394]. В электронном письме получателя просят раскрыть и/или подтвердить определенную конфиденциальную информацию. Многие жертвы следуют совету и раскрывают информацию, позволяя злоумышленникам делать онлайновые переводы и пр.[395].

В прошлом уголовные преступления, включающие подлог с использованием компьютера, были редкостью, так как большинство правовых документов были материальными. Цифровые документы играют все более важную роль и используются все чаще. Замена классических документов цифровыми поддерживается законными средствами, например, законно подтверждая право цифровой подписи (см. Рисунок 16).

Преступники всегда старались подделывать документы. С цифровой подделкой, цифровые документы теперь можно копировать без потери качества и легко их подделывать. Судебным экспертам трудно доказать цифровые махинации, если не используются технические средства защиты[396] для защиты документов от подделки[397].

---

388 For an overview of estimated losses, see *Reich*, "Advance Fee Fraud Scams in-country and across borders", "Cybercrime & Security", IF-1, page 3 et seqq.

389 For more information see the Ultrascan Survey "419 Advance Fee Fraud", version 1.7, 19.02.2008, available at: http://www.ultrascan.nl/assets/applets/2007_Stats_on_419_AFF_feb_19_2008_version_1.7.pdf.

390 See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

391 Regarding phishing, see *Dhamija/Tygar/Hearst*, "Why Phishing Works", available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; "Report on Phishing", A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: http://www.usdoj.gov/opa/report_on_phishing.pdf

392 The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und REcht, 2005, page 606; *Ollmann*, "The Phishing Guide Understanding & Preventing Phishing Attacks", available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

393 "Phishing" scams show a number of similarities to spam e-mails. It is likely that those organised crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see above: Chapter 2.5.g.

394 Regarding related trademark violations, see above: Chapter 2.6.2.

395 For more information about phishing scams see below: Chapter 2.8.4.

396 One technical solution to ensure the integrity of data is the use of digital signatures.

397 For case studies, see: *Sieber*, Council of Europe Organised Crime Report 2004, page 94.

2.7.3 Кража идентичности

Понятие кража идентичности, которое используется сознательно или бессознательно, – это описание преступного деяния по мошенническому получению и использованию идентичности личности[398]. Эти действия могут осуществляться без помощи технических средств[399], а также с использованием интернет технологии[400].

В целом такое преступление, как кража идентичности состоит из трех разных этапов[401]:

- На первом этапе преступник добывает информацию об идентичности. Эта часть преступления может, например, осуществляется с помощью вредоносных программ или фишинг-атак.
- Второй этап характеризуется взаимодействием с информацией об идентичности до ее использования при совершении преступлений[402]. Примером может служить продажа информации об идентичности[403]. Информация с кредитной карты, к примеру, стоит более 60 долл. США[404].
- Третий этап заключается в использовании информации об идентичности при совершении преступления. В большинстве случаев доступ к данным идентичности толкает преступника к совершению новых преступлений[405]. Поэтому преступники не фокусируются на содержании используемых данных, а используют возможность применить их для совершения преступлений. Примером такого преступления может быть подделка документов, удостоверяющих личность, или мошенничество с кредитными картами[406].

Способы, применяемые для получения данных в рамках первого этапа, охватывают широкий диапазон действий. Преступник может использовать физические способы, например, красть компьютерные запоминающие устройства, хранящие данные об идентичности, просматривание мусора ("копание в мусоре")[407] или воровать почту[408]. Кроме того, они могут использовать поисковые системы для поиска данных об идентичности. "Googlehacking" или "Googledorks" – термины, описывающие применение сложных поисковых запросов для фильтрации большого количества результатов поиска информации, связанной с вопросами компьютерной безопасности, а также частной информации, которая может быть использована мошенниками при краже идентичности. Одной из целей преступника может быть, к примеру, поиск

---

398 *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 39, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; Regarding the different definitions of Identity Theft see: *Gercke*, Internet-related Identity Theft, 2007, available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

399 One of the classic examples is the search for personal or secret information in trash or garbage bins ("dumpster diving"). For more information about the relation to Identity Theft see: Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

400 Javelin Strategy & Research 2006 Identity Fraud Survey points out that although there were concerns over electronic methods of obtaining information, most thieves still obtain personal information through traditional rather than electronic channels. In the cases where the methods were known, less than 15% obtained online by electronic means. See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.

401 *Gercke*, Internet-related Identity Theft, 2007, available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; For an approach to divide between four phases see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 et seq., available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

402 In some cases perpetrators used the data they obtained to hide their real identity. Regarding this aspect see: *Gercke*, Internet-related Identity Theft, 2007, available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

403 *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf.

404 See: 2005 Identity Theft: Managing the Risk, Insight Consulting, page 2, available at: http://www.insight.co.uk/files/whitepapers/Identity%20Theft%20(White%20paper).pdf.

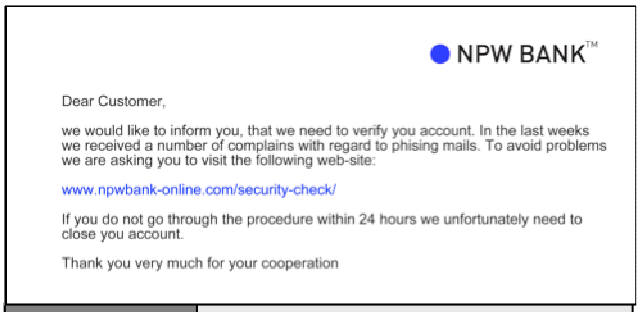
405 Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf .

406 Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

407 Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf; *Paget*, Identity Theft – McAfee White Paper, page 6, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

408 This method is not considered as an Internet-related approach.

незащищенных паролем систем для получения данных из этой системы[409]. Отчеты выявляют риски, которые возникают при легальном использовании поисковых систем в незаконных целях[410]. Аналогичные проблемы касаются и файлообменных систем. Конгресс США недавно обсуждал возможность использования файлообменных систем для получения личной информации, которая может быть использована при краже идентичности[411]. Кроме того, преступники могут использовать сотрудников организаций, которые имеют доступ к хранению информации об идентичности, чтобы завладеть ею. Обзор[412] компьютерных преступлений и безопасности ИКБ 2007 г. показывает, что более 35% опрошенных приписывают более 20% потерь своих организаций их сотрудникам. Наконец, преступники могут использовать психологические приемы, для того чтобы убедить жертву раскрыть личную информацию. В последние годы преступники разработали эффективные схемы мошенничества для получения секретной информации, например, информации о банковском счете и данные кредитной карты, управляя пользователями с помощью психологических приемов (см. Рисунок 17[413]).


NPW BANK™

Dear Customer,

we would like to inform you, that we need to verify you account. In the last weeks we received a number of complains with regard to phising mails. To avoid problems we are asking you to visit the following web-site:

www.npwbank-online.com/security-check/

If you do not go through the procedure within 24 hours we unfortunately need to close you account.

Thank you very much for your cooperation

Рисунок 17

Почтовые сообщения фишинга были использованы для получения секретной информации, такой как номер счета, пароль и номера операции, от объекта нападения. Эта информация может быть использована преступниками для совершения преступлений.

Виды данных, интересующих преступников, меняются[414]. Наиболее важными данными являются:

- **Номер социального страхования (SSN) или номер паспорта**. К примеру, номер социального страхования, используемой в США, является классическим примером того вида данных об идентичности, который интересует преступников. Несмотря на то, что SSN был создан для ведения точного учета дохода, в настоящее время он широко используется для идентификации[415]. Преступники могут использовать SSN или полученные паспортные данные, чтобы открыть финансовые счета, присвоить существующий финансовый счет, взять кредит или скрыться от долгов[416].

- **Дата рождения, адрес и номер телефона**. Эти данные, как правило, могут быть использованы для кражи идентичности, если они объединены с другими видами информации, например SSN[417]. Доступ к таким дополнительным данным, как дата рождения и адрес может помочь преступнику обойти процесс проверки. Одной из наибольших опасностей, связанной с этой информацией, является тот факт, что в настоящее время она общедоступна в интернете, либо добровольно опубликована на различных форумах, связанных с идентичностью[418], либо основана на законных требованиях, как отпечаток на веб-сайтах[419].

---

409 For more information see: *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Dornfest/Bausch/Calishain*, Google Hacks: Tips & Tools for Finding and Using the World's Information, 2006.

410 See: *Nogguchi*, Search engines lift cover of privacy, The Washington Post, 09.02.2004, available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

411 See: Congress of the United States, Committee on Oversight and Government Reform, 17.10.2007, available at: http://oversight.house.gov/documents/20071017134802.pdf.

412 The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of Cybercrime businesses. It is based on the responses of 494 computer security practitioners from in U.S corporations, government agencies and financial institutions. The Survey is available at: http://www.gocsi.com/.

413 See *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: http://www.securityfocus.com/infocus/1527.

414 For more details see: *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 et seq.

415 *Garfinkel*, Database nation: The Death of privacy in the 21st Century, 2000, page 33-34; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

416 See *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: http://www.privacyrights.org/ar/id_theft.htm.

417 *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005, page 6; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: http://www.privacyrights.org/ar/id_theft.htm.

418 Examples is the online community Facebook, available at http://www.facebook.com.

419 See for example Art. 5 of the Directive 2000/31/Ec Of The European Parliament And Of The Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

- **Пароль к нефинансовым учетным записям**. Доступ к паролю к учетным записям позволяет преступникам изменить настройки учетной записи и использовать ее в своих целях[420]. К примеру, они могут взять учетную запись электронной почты и использовать ее для отправки писем с незаконным содержанием или могут взять учетную запись пользователя на аукционе и использовать ее для продажи краденного[421].
- **Пароль к финансовым счетам**. Как и SSN, информация, относящаяся к финансовым счетам, является популярной целью для кражи идентичности. К ней относятся чековые и сберегательные счета, кредитные карты, дебетовые карты и информация о финансовом планировании. Подобная информация является важным источником для кражи идентичности при совершении финансовых киберпреступлений.

Кража идентичности является серьезной и растущей проблемой[422]. Последние данные свидетельствуют о том, что в первой половине 2004 года 3% домохозяйств США стали жертвой кражи идентичности[423]. В Соединенном Королевстве кражи идентичности обходятся британской экономике в 1,3 миллиарда фунтов стерлингов ежегодно[424]. Оценки потерь от краж идентичности в Австралии варьируются от менее 1 миллиарда долл. США до более 1,3 миллиарда долл. США в год[425]. Исследование мошеннических действий с идентичностью 2006 года оценивает потери США в 2005 году в 56,6 миллиардов долл. США[426]. Убытки могут быть не только финансовыми, но могут включать ущерб репутации[427]. В действительности, многие жертвы не сообщают о таких преступлениях, в то время как финансовые учреждения зачастую не желают обнародовать печальный опыт клиентов. Фактическое число случаев кражи идентичности, вероятно, намного превышает число зарегистрированных потерь[428].

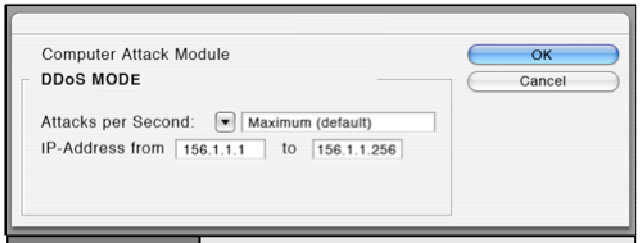


Рисунок 18

Доступно несколько инструментов, позволяющих злоумышленникам автоматизировать атаки на все компьютерные системы при помощи IP-адресов в пределах указанного IP-диапазона. При помощи таких программ возможно атаковать сотни компьютерных систем за несколько часов.

Кража идентичности основана на том факте, что имеется несколько способов установить личность пользователей через интернет. Легче определять людей в реальном мире, но большинство видов онлайновой идентификации являются более сложными. Сложные средства идентификации, например, с использованием биометрической информации, являются дорогостоящими и используются не везде. Существуют некоторые ограничения онлайновой деятельности, делающие кражу идентичности легкой и выгодной[429].

2.7.4 Неправильное использование устройств

Киберпреступление можно совершить при помощи всего лишь простейшего оборудования[430]. Для совершения таких преступлений, как онлайновые клевета или мошенничество, не требуется ничего, кроме компьютера и доступа в интернет, и они могут совершаться из общественного интернет-кафе. Более сложные преступления могут совершаться при помощи специальных программных инструментов.

---

420 Putting an End to Account-Hijacking identity Theft, page 10, Federal Deposit insurance Corporation, 2004, available at: http://www.fdic.gov/consumers/consumer/idtheftstudy/identity_theft.pdf.

421 Regarding forensic analysis of e-mail communication see: *Gupta*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

422 "Identity Theft, Prevalence and Cost Appear to be Growing", GAO-02-363.

423 United States Bureau of Justice Statistics, 2004, available at http://www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

424 See Identity Theft: Do you know the signs?, The Fraud Advisory Panel, page 1, available at: http://www.fraudadvisorypanel.org/newsite/PDFs/advice/Identity%20Theft%20Final%20Proof%2011-7-03.pdf.

425 *Paget*, Identity Theft – McAfee White Paper, page 10, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

426 See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf.

427 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* "Identity Theft – A discussion paper", 2004, page 5, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

428 The United States Federal Bureau of Investigation (FBI) requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. The Head of the FBI office in New York is quoted as saying: "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack". See: Heise News, available at: http://www.heise-security.co.uk/news/80152.

429 See: *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* "Identity Theft – A discussion paper", 2004, page 5, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

430 The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: Chapter 3.2.h.

Инструменты, требуемые для совершения комбинированных преступлений, легко доступны через интернет[431], часто бесплатно. Более сложные инструменты стоят несколько тысяч долларов[432]. При помощи таких программных инструментов злоумышленники могут атаковать другие компьютерные системы простым нажатием клавиши (см. Рисунок 18). Обычные атаки теперь малоэффективны, так как компании, производящие программы защиты, в настоящее время могут и подготовлены для отражения простых хакерских атак. Высокоуровневые атаки часто разрабатываются специально для определенных целей[433]. Программные инструменты существуют для[434]:

- проведения DoS атак[435];
- создания компьютерных вирусов;
- дешифрования зашифрованных сообщений; и
- незаконного доступа к компьютерным системам.

Второе поколение программных инструментов теперь автоматизировало множество киберафер и позволило злоумышленникам осуществлять множественные атаки за малое время. Программные инструменты также упростили атаки, позволяя совершать киберпреступления менее искушенным пользователям компьютеров. Доступны наборы инструментов для спама, которые позволяют практически каждому рассылать электронные письма со спамом[436]. В настоящее время существуют программные инструменты, которые можно использовать для скачивания и закачивания файлов из файлообменных систем. С большей доступностью специально разработанных программных инструментов, число возможных злоумышленников существенно увеличилось. Различные национальные и международные законотворческие инициативы были предприняты в отношении программных инструментов для киберафер, например, преследуя судебным порядком их создание, продажу или обладание[437].

2.8 Комбинированные преступления

Существует целый ряд терминов, используемых для описания сложных мошеннических действий, охватывающий ряд различных правонарушений. Примеры включают:

- кибертерроризм;
- отмывание денег с использованием компьютерных технологий; и
- фишинг.

2.8.1 Кибертерроризм

Ранее в 1990-х годах дискуссии по поводу использования сети террористическими организациями делали акцент на сетевых атаках против важных объектов инфраструктуры, таких как

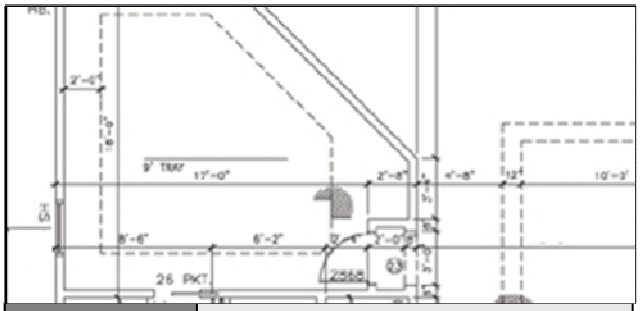


Рисунок 19

Интернет является важным источником информации, включая информацию (например, архитектурные планы) о потенциальных целях (таких, как общественные здания) - можно найти, например, веб-сайт архитектора и т. д.

---

431 "Websense Security Trends Report 2004", page 11, available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; "Information Security - Computer Controls over Key Treasury Internet Payment System", GAO 2003, page 3, available at: http://www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe "Organised Crime Report 2004", page 143.

432 For an overview about the tools used, see *Ealy*, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", available at: http://www.212cafe.com/download/e-book/A.pdf. Regarding the price of keyloggers (200 – 500 US Dollar) see: Paget, Identity Theft, White Paper, McAfee, 2007, available at: http://www.mcafee.com/us/threat_center/white_paper.html.

433 See above: Chapter 2.4.1.

434 For more examples, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 23 et seq., available at: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf; *Berg*, "The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies", Michigan Law Journal 2007, page 21, available at: http://www.michbar.org/journal/pdf/pdf4article1163.pdf.

435 DoS is an acronym for Denial-of-Service attack. For more information, see above : Chapter 2.4.e.

436 These generally contain two elements: Software that automates the process of sending out e-mails by avoiding techniques that enable e-mail providers to identify spam e-mails and a database with thousands or even millions of e-mail addresses. For more information, see: "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond", page 25, available at: http://www.antiphishing.org/reports/APWG_CrimewareReport.pdf.

437 For more details, see below: Chapter 6.1.13.

транспорт и энергоснабжение ("кибертерроризм"), и использование информационных технологий в вооруженных конфликтах ("кибервойна"[438]). Успех вирусных атак и атак сетевого робота ясно продемонстрировал недостатки в безопасности сети. Успешные интернет-атаки со стороны террористов возможны[439], но трудно оценить значимость угроз[440], и в то же время степень взаимосвязи мало сравнима с текущим состоянием и очень вероятно, что наряду с заинтересованностью государств продолжать замалчивать успешные атаки, это одна из главных причин того, почему о таких инцидентах сообщалось крайне мало. По крайней мере в прошлом, именно поэтому падение деревьев создавало большую опасность для энергоснабжения, чем успешные хакерские атаки[441].

Это положение изменилось после нападения 11 сентября. Началось интенсивное обсуждение вопросов об использовании ИКТ террористами[442]. Обсуждению способствовала сообщения[443] о том, что в процессе подготовки к нападению преступники использовали интернет[444]. Несмотря на то, что нападение не являлось кибератакой, а группа, осуществившая нападение 11 сентября, не проводила интернет-атаки, интернет сыграл определенную роль в подготовке этого преступления[445]. В этом контексте были открыты различные способы, которыми террористические организации используют интернет[446]. Сегодня известно, что террористы используют ИКТ и интернет для:

- пропаганды;
- сбора информации;
- подготовки нападений в реальном мире;
- публикации учебных материалов;
- связи;
- финансирования террористов;
- атак на важнейшую инфраструктуру.

Этот сдвиг центра внимания обсуждения оказал положительное действие на исследования, связанные с кибертерроризмом, поскольку он высветил неизвестные до этого области террористической деятельности.

---

438 *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 et. seq.

439 *Rollins/ Wilson*, "Terrorist Capabilities for Cyberattack", 2007, page 10, available at: http://www.fas.org/sgp/crs/terror/RL33123.pdf.

440 The CIA pointed out in 2002 that attacks against critical infrastructure in the United States will become an option for terrorists. Regarding the CIA position, see: *Rollins/Wilson*, "Terrorist Capabilities for Cyberattack, 2007", page 13, available at: http://www.fas.org/sgp/crs/terror/RL33123.pdf. However, the FBI has stated that there is presently a lack of capability to mount a significant cyber-terrorism campaign. Regarding the FBI position, see: *Nordeste/Carment*, "A Framework for Understanding Terrorist Use of the Internet, 2006", available at: http://www.csis-scrs.gc.ca/en/itac/itacdocs/2006-2.asp

441 See: Report of the National Security Telecommunications Advisory Committee - Information Assurance Task Force - Electric Power Risk Assessment, available at: http://www.aci.net/kalliste/electric.htm.

442 See: *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity"; http://www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 et. seq.; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Denning*, "Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy", in Arquilla/Ronfeldt, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 et seqq., available at: http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, "Cyberterrorism, Are We Under Siege?", American Behavioral Scientist, Vol. 45 page 1033 et seqq; United States Department of State, "Pattern of Global Terrorism, 2000", in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism", available at: http://www.symantec.com/avcenter/reference/cyberterrorism.pdf; US-National Research Council, "Information Technology for Counterterrorism: Immediate Actions and Future Possibilities", 2003, page 11 et seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/ lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

443 See: *Rötzer*, Telepolis News, 4.11.2001, available at: http://www.heise.de/tp/r4/artikel/9/9717/1.html.

444 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail see *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;

445 CNN, News, 04.08.2004, available at: http://www.cnn.com/2004/US/08/03/terror.threat/index.html.

446 For an overview see: *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 et. seq.;

Но несмотря на важность комплексного подхода, угрозы, связанные с интернет-атаками на важнейшую инфраструктуру, не должны выйти из центра внимания обсуждения. Уязвимость и растущая зависимость[447] от информационных технологий заставляет включать в стратегии по предотвращению и борьбе с кибертерроризмом атаки на важнейшую инфраструктуру, связанную с интернетом.

Но несмотря на более интенсивные исследования, борьба с кибертерроризмом остается трудной. Сравнение различных национальных подходов показывает, что в стратегиях много общего[448]. Одной из причин такого развития является тот факт, что международное сообщество признало, что угрозы международного терроризма требуют глобальных решений[449]. Но в настоящее время непонятно, является ли такой подход успешным, или различные правовые системы и различных культурные традиции требуют различных решений. Оценка этого вопроса ставит уникальные проблемы, поскольку, за исключением сообщений о крупных инцидентах, у нас есть очень мало данных, которые могут быть использованы для научного анализа. Те же трудности возникают в связи с определением уровня угрозы, связанной с использованием террористическими организациями информационных технологий. Эта информация очень часто является секретной и поэтому доступна только для разведки[450]. Еще не достигнут даже консенсус по термину "терроризм"[451]. Доклад CRS для Конгресса США, к примеру, утверждает, что тот факт, что один террорист забронировал авиабилет в США через интернет, является доказательством того, что террористы используют интернет при подготовке своих нападений[452]. Этот довод представляется не совсем корректным, так как бронирование билетов на рейс не становится деятельностью, связанной с терроризмом, только потому, что она осуществляется террористом.

Пропаганда

В 1998 году только 12 из 30 иностранных террористических организаций, перечисленных в Государственном Департаменте Соединенных Штатов, поддерживали веб-сайты с целью информирования общественности о своей деятельности[453]. В 2004 году Американский институт мира сообщил, что почти все террористические организации поддерживают веб-сайты, среди них Хамас, Хезболла, РКК и Аль-Каида[454]. Террористы также начали использовать видео сообщество, например YouTube, для распространения видеосообщений и пропаганды[455]. Использование веб-сайтов и других форумов является признаком более профессионального внимания диверсионных групп к связям общественностью[456]. Веб-сайты и другие средства массовой информации используются для распространения пропаганды[457], описания и публикаций[458], обоснования своей деятельности и вербовки[459] новых и связи с существующими членами и источниками финансирования[460]. В последнее время веб-сайты были использованы для распространение видеозаписей казней[461].

---

447 *Sofaer/Goodman*, "Cybercrime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf.

448 Regarding different international approaches as well as national solutions see: *Sieber* in Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007;

449 One example for such approach is the amendment of the European Union Framework Decision on combating terrorism, COM(2007) 650.

450 Regarding attacks via the Internet: *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001, page 12; *Vatis* in Cyber Attacks During the War on Terrorism, page 14ff.; *Clark*, Computer Security Officials Discount Chances of 'Digital Pearl Harbour', 2003; USIP Report, Cyberterrorism, How real is the threat, 2004, page 2; *Lewis*, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats; *Wilson* in CRS Report, Computer Attack and Cyber Terrorism - Vulnerabilities and Policy Issues for Congress, 2003.

451 See for example *Record*, Bounding the global war on terrorism, 2003, available at: http://strategicstudiesinstitute.army.mil/pdffiles/PUB207.pdf.

452 *Wilson* in CRS Report, Computer Attack and Cyber Terrorism - Vulnerabilities and Policy Issues for Congress, 2003, page 4.

453 ADL, Terrorism Update 1998, available at: http://www.adl.org/terror/focus/16_focus_a.asp.

454 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 3. Regarding the use of the Internet for propaganda purposes see as well: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

455 Regarding the use of YouTube by terrorist organisations, see Heise News, news from 11.10.2006, available at: http://www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

456 *Zanini/Edwards*, "The Networking of Terror in the Information Age", in Networks and Netwars: The Future of Terror, Crime, and Militancy, 2001, page 42.

457 United States Homeland Security Advisory Council, Report of the Future of Terrorism, 2007, page 4.

458 Regarding the justification see: *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: http://www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf.

459 *Brachman*, High-Tech Terror: Al-Qaeda's Use of New Technology, The Fletcher Forum of World Affairs, Vol. 30:2, 2006, page 149 et. seqq.

460 See: *Conway*, "Terrorist Use of the Internet and Fighting Back", "Information and Security", 2006, page 16.

461 Videos showing the execution of American citizens Berg and Pearl were made available on websites. See *Weimann* in the USIP Report, "How Terrorists use the Internet", 2004, page 5.

Сбор информации

Значительный объем информации о возможных жертвах доступен в интернете[462]. К примеру, архитекторы, участвующие в строительстве общественных зданий, часто публикуют планы зданий на своих веб-сайтах (см. Рисунок 21). Сегодня в различных услугах интернета бесплатно доступны спутниковые фотографии с высоким разрешением, те самые, которые годы назад были доступны только для очень немногих военных институтов в мире[463]. Кроме того, были обнаружены инструкции о том, как сделать бомбу, и даже виртуальные учебные лагеря, предоставляющие инструкции по использованию оружия в форме дистанционного электронного обучения[464]. Кроме того, секретная или конфиденциальная информация, не защищенная должным образом от поисковых роботов, может быть доступна через поисковые системы[465]. В 2003 году Министерство обороны США сообщило, что учебное пособие, связанное с Аль-Каидой, содержит информацию о том, какие открытые источники могут быть использованы для поиска детальной информации о потенциальных целях[466]. В 2006 году New York Times сообщила, что основные сведения, связанные с созданием ядерного оружия, были опубликованы на веб-сайте правительства во время представления доказательств о намерениях Ирака в разработке ядерного оружия[467]. Аналогичный случай был зарегистрирован в Австралии, где подробная информация о потенциальных целях террористических атак была размещена на веб-сайтах правительства[468]. В 2005 году в Германии пресса сообщила об обнаружении разведчиками того факта, что пособия по созданию взрывчатых веществ были скачаны из интернета на компьютер двумя подозреваемыми, предпринявшими попытку нападения на общественный транспорт с использованием самодельных бомб[469].

Подготовка нападений в реальном мире

Существуют различные способы использования террористами информационных технологий при подготовке нападения. Отправка сообщений по электронной почте или публикация в форумах являются примерами, которые будут обсуждаться с точки зрения связи[470]. В настоящее время обсуждаются более прямые пути онлайновой подготовки. Опубликованы доклады, отмечающие, что террористы при подготовке нападения используют онлайновые игры[471]. Существуют различные онлайновые игры, способные имитировать реальный мир. Пользователь таких игр может использовать персонажей (аватар) для действий в виртуальном мире. Теоретически такие онлайновые игры могут быть использованы для моделирования нападений, но пока не определено, в какой степени онлайновые игры уже применяются в этой деятельности[472].

Публикация учебных материалов

Интернет может быть использован для распространения учебных материалов, таких как инструкции по использованию оружия и о том, как выбирать цели. Такой материал доступен в больших объемах из онлайн-источников[473]. В 2008 году западные спецслужбы обнаружили интернет-сервер, служивший основой для

---

462 Regarding the related challenges see *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 292.

463 *Levine*, Global Security, 27.06.2006, available at: http://www.globalsecurity.org/org/news/2006/060627-google-earth.htm.; Regarding the discovery of a secret submarine on a satellite picture provided by a free of charge Internet Service see: Der Standard Online, Goolge Earth: Neues chinesisches Kampf-Uboot entdeckt, 11.07.2007, available at: http://www.derstandard.at/?url/?id=2952935.

464 For further reference see: *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, 292.

465 For more information regarding the search for secret information with the help of search engines, see *Long, Skoudis, van Eijkelenborg*, "Google Hacking for Penetration Testers".

466 "Using public sources openly and without resorting to illegal means, it is possible to gather at least eighty per cent of information about the enemy." For further information, see *Conway*, "Terrorist Use of the Internet and Fighting Back", Information & Security, 2006, Page 17.

467 See *Broad*, US Analysts Had flagged Atomic Data on Web Site, New York Times, 04.11.2006.

468 *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 18,

469 See Sueddeutsche Zeitung Online, BKA findet Anleitung zum Sprengsatzbau, 07.03.2007, available at: http://www.sueddeutsche.de/deutschland/artikel/766/104662/print.html.

470 See below.

471 See US Commission on Security and Cooperation in Europe Briefing, 15.05.2008, available at: http://csce.gov/index.cfm?FuseAction=ContentRecords.ViewTranscript&ContentRecord_id=426&ContentType=H,B&ContentRecordType=B&CFID=18849146&CFTOKEN=53; O'Brian, Virtual Terrorists, The Australian, 31.07.2007, available at: http://www.theaustralian.news.com.au/story/0,25197,22161037-28737,00.html*; O'Hear*, Second Life a terrorist camp?, ZDNet,

472 Regarding other terrorist related activities in online games see: *Chen/Thoms*, Cyber Extremism in Web 2.0 - An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, page 98 et seqq.

473 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; United States Homeland Security Advisory Council, Report of the Future of Terrorism Task Force, January 2008, page 5; *Stenersen*, The Internet: A Virtual Training Camp? In Terrorism and Political Violence, 2008, page 215 et seq.

обмена учебными материалами, а также для связи[474]. Сообщается о работе различных сайтов, управляемые террористическими организациями в целях координации деятельности[475].

Связь

Использование информационных технологий террористическими организациями не ограничивается запуском веб-сайтов и поиском в базах данных. В рамках расследований после нападений 11 сентября было сообщено о том, что для координации своих нападений террористы использовали электронную почту[476]. В прессе сообщалось о передаче по электронной почте подробных инструкций о целях и числе нападающих[477]. С помощью технологии шифрования и средств анонимной связи другой участник может еще более увеличить трудности в идентификации и мониторинге террористических связей.

Финансирование терроризма

Большинство террористических организаций зависит от финансовых ресурсов, которые они получают от третьих сторон. Отслеживание этих финансовых операций стало одним из основных подходов в борьбе с терроризмом после нападений 11 сентября. Одной из главных трудностей в этом отношении является тот факт, что финансовые ресурсы, необходимые для проведения нападений, не обязательно велики[478]. Существует несколько способов использования интернета для финансирования террористической деятельности. Террористические организации могут пользоваться электронными платежными системами для внесения денежных средств онлайн[479]. Они могут использовать веб-сайты для публикации информации о том, как внести денежные средства, например на банковский счет, который должен быть использован для сделок. Одним из примеров такого подхода является организации "Хизб аль-Тахрир", которая опубликовала сведения о банковском счете для потенциальных спонсоров[480]. Другой способ заключается в осуществлении онлайновых денежных пожертвований с помощью кредитных карт. Ирландская республиканская армия (ИРА) была одной из первых террористических организаций, которая предложила пожертвования с помощью кредитной карты[481]. Оба подхода имеют риск того, что публикуемая информация может быть открыта и использована для отслеживания финансовых операций. Вероятно именно поэтому анонимные электронные платежные системы становятся все более популярными. Для того чтобы избежать обнаружения, террористические организации пытаются скрыть свою деятельность путем привлечения не вызывающих подозрений игроков, таких как благотворительные организации. Другим связанным с интернетом подходом является работа фальшивых интернет-магазинов. Относительно просто создать онлайн-магазин в интернет. Одним из самых больших преимуществ сети является то, что предприятия могут работать по всему миру. Доказать, что финансовые операции, имевшие место на тех сайтах, являлись не обычными покупками, а денежными пожертвованиями, довольно сложно. Необходимо расследовать каждую сделку, что может быть затруднительно, если интернет-магазин работает в другой юрисдикции или были использованы анонимные платежные системы[482].

---

474 *Musharbash*, Bin Ladens Intranet, Der Spiegel, Vol. 39, 2008, page 127.

475 *Weimann*, How Modern Terrorism uses the Internet, 116 Special Report of the United States Institute of Peace, 2004, page 10.

476 The 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, 2007, page 249.

477 The text of the final message was reported to be: “The semester begins in three more weeks. We’ve obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering.“ The name of the faculties was apparently the code for different targets. For more detail see *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of “cyberplanning”, 2003, available at: http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: http://www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position=;

478 The Commission analyzing the 9/11 attacks calculated that the costs for the attack could have been between 400.000 and 500.000 USD. See 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, page 187. Taking into account the duration of the preparation and the number of people involved the cost per person have been relatively small. Regarding the related challenges see as well *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.

479 See in this context: *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

480 *Weimann* in USIP Report, How Terrorists use the Internet, 2004, page 7.

481 See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4,

482 Regarding virtual currencies see *Woda*, Money Laundering Techniques with Electronic Payment Systems in Information and Security 2006, page 39.

Нападения на важнейшие инфраструктуры

В дополнение к обычным компьютерным преступлениям, таким как мошенничество и кража идентичности, целью террористов может стать нападение на важнейшие информационные инфраструктуры. Растущая зависимость от информационных технологий делает важнейшие инфраструктуры более уязвимыми для нападения[483]. Это особенно важно в связи с нападениями на взаимосвязанные системы, которые связаны компьютерными сетями и сетями связи[484]. В этих случаях нарушения, вызванные сетевой атакой, происходят вместе с отказами одиночных систем. Даже короткие перерывы в предоставлении услуг могут привести к огромным финансовым потерям для предприятия электронной коммерции, не только для гражданских служб, но и для военной инфраструктуры и служб[485]. Расследование или даже предотвращение таких атак представляют собой уникальные задачи[486]. В отличие от физического нападения, преступникам не обязательно присутствовать там, где происходит нападение[487]. И при проведении этого нападения преступники могут использовать средства анонимной связи и технологии шифрования, для того чтобы скрыть свою идентичность[488]. Как было отмечено выше, расследование таких атак требует специальных процедурных инструментов, технологий исследования и обучения персонала[489].

Широко признано, что важнейшие инфраструктуры являются потенциальной целью террористических атак, так как они, по определению, имеют жизненно важное значение для устойчивости и стабильности государства[490]. Инфраструктура считается важнейшей, если вывод ее из строя или ее уничтожение оказали бы ослабляющее воздействие на оборону или экономическую безопасность государства[491]. В частности, таковыми являются: электроэнергетические системы, системы связи, хранение и перевозка газа и нефти, банковское дело и финансы, транспорт, системы водоснабжения и аварийные службы. Степень гражданских беспорядков, вызванных нарушением услуг в результате урагана Катрина в США, подчеркивает зависимость общества от наличия этих услуг[492].

Уязвимость важнейших объектов инфраструктуры в области сетевых атак может быть доказана путем выделения некоторых случаев, связанных с воздушным транспортом.

- Системы проверки большинства аэропортов в мире уже основаны на взаимосвязанных компьютерных системах[493]. В 2004 году компьютерный червь Sasser[494] инфицировал миллионы компьютеров по всему миру, в том числе компьютерных систем крупных авиакомпаний, что привело к отмене рейсов[495].

---

483 *Sofaer/Goodman*, "Cybercrime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, available at: http://media.hoover.org/documents/0817999825_1.pdf

484 *Lewis*, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December 2002.

485 *Shimeall/Williams/Dunlevy*," Countering cyber war", NATO review, Winter 2001/2002, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf

486 *Gercke*, The slow wake of a global approach against cybercrime, Computer und Recht International, 2006, page 140 et seq.

487 *Gercke*, The Challenge of fighting Cybercrime, Multimedia und Recht, 2008, page 293.

488 CERT Research 2006 Annual Report", page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf

489 Law Enforcement Tools and Technologies for Investigating Cyber Attacks, DAP Analysis Report 2004, available at: http://www.ists.dartmouth.edu/projects/archives/ISTSGapAnalysis2004.pdf.

490 *Brunst i*n Sieber/Brunst, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007.

491 United States Executive Order 13010 – *Critical Infrastructure Protection*. Federal Register, July 17,1996. Vol. 61, No. 138.

492 Critical Infrastructure Protection: Sector Plans and Sector Councils Continue to Evolve, GAO communication, July 2007, available at: http://www.gao.gov/new.items/d07706r.pdf.

493 *Kelemen*, Latest Information Technology Development in the Airline Industry, 2002, Periodicapolytechnica Ser. Transp. Eng., Vol. 31, No. 1-2, page 45-52, available at: http://www.pp.bme.hu/tr/2003_1/pdf/tr2003_1_03.pdf; *Merten/Teufel*, Technological Innovations in the Passenger Process of the Airline Industry: A Hypotheses Generating Explorative Study in O'Conner/Hoepken/Gretzel, Information and Communication Technologies in Tourism 2008.

494 Sasser B Worm, Symantec Quick reference guide, 2004, available at: http://eval.symantec.com/mktginfo/enterprise/other_resources/sasser_quick_reference_guide_05-2004.en-us.pdf.

495 *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; The Sasser Event: History and Implications, Trend Micro, June 2004, available at: http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/wp02sasserevent040812us.pdf.

- Сегодня значительное число билетов приобретается в режиме онлайн. Авиакомпании используют информационные технологии для различных операций. Все крупные авиакомпании предоставляют своим клиентам возможность купить билеты в режиме онлайн. Как и другие виды электронной коммерческой деятельности, эти онлайновые услуги могут быть мишенью для злоумышленников. Одним общим методом, используемым для атак на услуги интернет, является атака отказа в обслуживании (DoS[496]). В 2000 году в течение непродолжительного периода времени были предприняты несколько DoS атак в отношении хорошо известных фирм, таких как CNN, Ebay и Amazon[497]. В результате некоторые из услуг были недоступны в течение нескольких часов или даже дней[498]. Авиакомпании были также затронуты атаками DoS. В 2001 году объектом нападения стал веб-сайт Lufthansa[499].

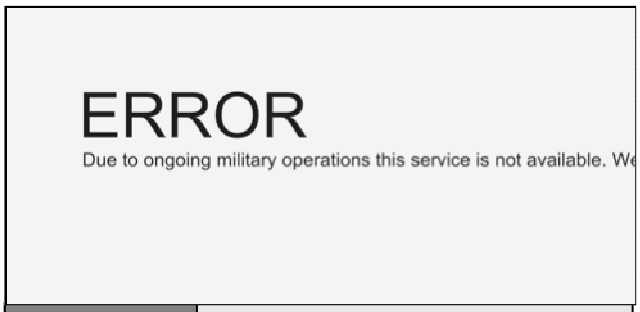


Рисунок 20

За последние годы интернет стал важной средой обмена информацией и пропаганды во время вооруженных конфликтов. Часто обсуждается, насколько возможна и/или целесообразна дезактивация некоторые услуг интернет во время прохождения ключевых этапов конфликта.

- Уязвимость систем управления полетом под контролем компьютера была продемонстрирована хакерской атакой на аэропорт Worcester в США в 1997 году[500]. Еще одной потенциальной мишенью для интернет-атак на важнейшие инфраструктуры являются системы управления полетами аэропортов. Во время хакерской атаки, правонарушитель дезактивировал телефонные услуги в башне аэропорта и выключил систему управления огнями взлетно-посадочной полосы[501].

2.8.2 Информационная война

Информационная война описывает использование ИКТ в области ведения боевых действий с использованием интернет. Она имеет ряд общих черт с кибертерроризмом[502]. Обсуждение первоначально фокусировалось на замещении классических военных действий нападениями с использованием компьютера или основанных на использовании компьютера[503]. Нападения, основанные на использовании сети, как правило дешевле, нежели традиционные военные операции[504], и могут быть осуществлены даже в малых государствах.

Защита от кибератак трудна. До настоящего времени опубликовано ограниченное число сообщений по замещению вооруженных конфликтов атаками, основанными на использовании интернета[505]. Текущие дискуссии сфокусированы на атаках на важнейшие инфраструктуры и контроле информации в ходе конфликта (см. Рисунок 20).

---

496 *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, "Analysis of a Denial of Service Attack on TCP", 1997; *Houle/Weaver*, "Trends in Denial of Service Attack Technology", 2001, available at: http://www.cert.org/archive/pdf/DoS_trends.pdf.

497 *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.

498 *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq.; *Lemos*, Web attacks: FBI launches probe, ZDNet News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html.

499 *Gercke*, The Decision of the District Court of Frankfurt in the Lufthansa Denial of Service Case, Multimedia und Recht, 2005, page 868-869.

500 Improving our Ability to Fight Cybercrime: Oversight of the National Infrastructure Protection Center, Hearing before the Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary United States Senate One Hundred Seventh Congress First Session, July 2001, Serial No. J–107–22, available at: http://cipp.gmu.edu/archive/215_S107FightCyberCrimeNICPhearings.pdf.

501 Critical Infrastructure Protection, Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain, September 2007, GAO-07-1036, available at: http://www.gao.gov/new.items/d071036.pdf; *Berinato*, Cybersecurity – The Truth About Cyberterrorism, March 2002, available at: http://www.cio.com/article/print/30933.

502 See above: Chapter 2.8.1.

503 Regarding the beginning discussion about Cyberwarfare, see: *Molander/Riddile/Wilson*, "Strategic Information Warfare, 1996", available at: http://www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

504 *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996, page 15, available at: http://www.rand.org/pubs/monograph_reports/MR661/MR661.pdf.

505 *Shimeall/Williams/Dunlevy*, "Countering cyber war", NATO review, Winter 2001/2002, page 16, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf; *Yurcik/Sharma*, "Internet Hack Back as an Active Defense Strategy", 2005, available at: http://www.projects.ncassr.org/hackback/ccsa05.pdf.

В том, что касается как гражданской, так и военной связи, информационная инфраструктура является одной из ключевых мишеней вооруженных конфликтов. Тем не менее, остается неясным, могут ли подобные атаки осуществляться через интернет. Атаки на компьютерные системы Эстонии[506] и США[507] были связаны с информационной войной. Поскольку атаки невозможно отследить до официальных правительственных организаций с некоторой долей определенности, их трудно классифицировать как информационную войну. Нападения на инфраструктуру, осуществленные физически, например, с применением оружия и взрывчатых веществ, также трудно классифицировать как информационную войну[508].

Контроль информации всегда являлся важным вопросом в ходе вооруженных конфликтов, так как информацию можно использовать для влияния на общественность, как и на военнослужащих противника. Контроль информации через интернет будет становиться все более важным средством воздействия в ходе вооруженных конфликтов.

2.8.3 Отмывание денег с использованием компьютерных технологий

Интернет меняет отмывание денег. Для крупных сумм традиционные методы отмывания денег еще обладают целым рядом преимуществ, но интернет имеет несколько достоинств. Онлайновые финансовые услуги предлагают возможность очень быстрого выполнения многочисленных финансовых операций по всему миру. Интернет помогает преодолеть зависимость от физических денежных операций. Безналичные переводы заменили переводы наличных денег и стали первым шагом в устранении физической зависимости от денег, но строгие правила выявления подозрительных безналичных переводов вынудили злоумышленников разработать новые методы. Выявление подозрительных сделок в области борьбы с отмыванием денег основано на обязательствах финансовых учреждений, принимающих участие в сделке[509].

Отмывание денег в целом подразделяется на три стадии:

1 размещение;

2 расслоение (разбивка крупных сумм денег на более мелкие); и

3 суммирование.

Касательно размещения больших объемов наличных средств, использование интернета, возможно, не даст заметных преимуществ[510]. Вместе с тем, интернет особенно полезен для правонарушителей на стадии расслоения или маскировки. С этой точки зрения, расследования отмывания денег особенно трудны, когда лица, отмывающие деньги, используют для расслоения онлайновые казино (см. Рисунок 21[511]).

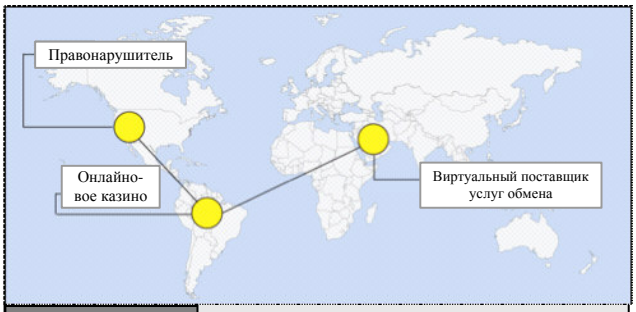


Рисунок 21

Рисунок выше иллюстрирует сочетание онлайновых казино и виртуальных валют в отмывании денег с использованием мошенниками интернета. Используя такие услуги, правонарушители могут затруднить правоохранительным органам отслеживание процессов перевода и идентификацию нарушителей.

Регулирование денежных переводов в настоящее время ограничено, и интернет дает правонарушителям возможность дешево и без налога перевести деньги за границу. Текущие трудности в расследовании методов отмывания денег с использованием интернет часто обусловлены использованием виртуальной валюты и онлайновых казино.

---

506 *Traynor,* "Russia accused of unleashing cyberwar to disable Estonia", The Guardian, 17.05.2007, available at: http://www.guardian.co.uk/russia/article/0,,2081438,00.html.

507 *Thornburgh*, "Inside the Chinese Hack Attack", Time, 25.08.2005, available at: http://www.time.com/time/nation/printout/0,8816,1098371,00.html.

508 One example is the intentional destruction of communication infrastructure by NATO forces during the war in the former Republic of Yugoslavia. Regarding this issue, see: http://www.nato.int/kosovo/press/p990506c.htm.

509 One of the most important obligations is the requirement to keep records and to report suspicious transactions.

510 Offenders may tend to make use of the existing instruments e.g., the service of financial organisations to transfer cash, without the need to open an account or transfer money to a certain account.

511 For case studies, see: "Financial Action Task Force on Money Laundering", "Report on Money Laundering Typologies 2000 – 2001", 2001, page 8.

1 Использование виртуальных валют

Одним из ключевых факторов в развитии виртуальных валют были микроплатежи, например, для загрузки из сети статей стоимостью 10 центов США или меньше, для которых проблематично использовать кредитную карту. С ростом спроса на микроплатежи были разработаны виртуальные валюты, в том числе "виртуальные золотые валюты". Виртуальные золотые валюты являются платежными системами, использующими счета, обеспеченные золотыми депозитами. Пользователи могут открыть электронный золотой счет в онлайновом режиме, зачастую без регистрации. Некоторые поставщики услуг даже разрешают прямой одноранговый (от лица к лицу) перевод или снятие наличных[512]. Правонарушители могут открыть электронные золотые счета в разных странах и комбинировать их, усложняя использование финансовых инструментов для отмывания денег и финансирования терроризма. Владельцы счетов могут также использовать неточную информацию при регистрации для скрытия своей идентичности[513].

2 Использование онлайновых казино

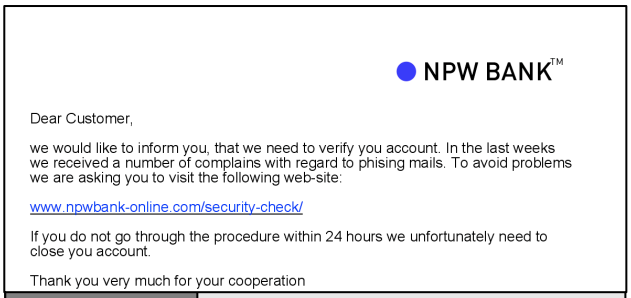
В отличие от реального казино для открытия онлайнового казино не требуется больших финансовых вложений[514]. Кроме того, положениях об онлайновых и реальных казино часто различаются в разных странах[515]. Отследить денежные переводы и доказать, что средства были не выиграны, а отмыты, можно только если казино хранит записи и предоставляет их органам охраны правопорядка.

Текущие правовое регулирование финансовых услуг с использованием интернета не столь строгое, как традиционное финансовое законодательство. Помимо пробелов в законодательстве, трудности в регулировании возникнут в связи с:

- трудностью проверки клиента: точность проверки может быть скомпрометирована, если поставщик финансовых услуг и клиент никогда не встречались[516];
- отсутствием личного контакта: трудно применять традиционные процедуры "знай своего клиента"; и
- тем, что интернет-переводы часто связаны с участием зарубежных поставщиков в различных странах;
- отсутствием закона/уголовного кодекса для мониторинга некоторых документов, что особенно сложно, когда поставщики позволяют клиентам переводить средства по одноранговой модели.

2.8.4 Фишинг

Правонарушители разработали методы для получения личной информации от пользователей начиная от программ-шпионов[517] до "фишинговых"-атак[518]. "Фишинг" описывает действия, проводимые для раскрытия жертвой личной/секретной информации[519]. Существуют различные типы фишинговых атак[520], но фишинговые атаки с использованием электронной почты состоят их трех основных этапов. На первом этапе злоумышленники определяют законные компании, которые предлагают онлайновые услуги и общаются с клиентами в электронном виде, которых


NPW BANK™

Dear Customer,

we would like to inform you, that we need to verify you account. In the last weeks we received a number of complains with regard to phising mails. To avoid problems we are asking you to visit the following web-site:

www.npwbank-online.com/security-check/

If you do not go through the procedure within 24 hours we unfortunately need to close you account.

Thank you very much for your cooperation

Рисунок 22

Фишинговые сообщения электронной почты выглядят как сообщение электронной почты законной компании, для того чтобы побудить жертву раскрыть секретную информацию. Очень часто правонарушители нацелены на клиентов финансовых учреждений.

512 See: *Woda*, "Money Laundering Techniques With Electronic Payment Systems", Information & Security, Vol. 18, 2006, page 40.
513 Regarding the related challenges see below: Chapter 3.2.l.
514 The costs of setting up an online casino are not significantly larger than other e-commerce businesses.
515 Regarding approaches to the criminalisation of illegal gambling, see below: Chapter 6.1.j.
516 See: Financial Action Task Force on Money Laundering, "Report on Money Laundering Typologies 2000 – 2001", 2001, page 2.
517 Regarding the threat of spyware, see *Hackworth*, "Spyware, Cybercrime and Security", IIA-4.
518 Regarding the phenomenon of phishing, see. *Dhamija/Tygar/Hearst*, "Why Phishing Works", available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; "Report on Phishing", A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, 2006, available at: http://www.usdoj.gov/opa/report_on_phishing.pdf
519 The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, "The Phishing Guide Understanding & Preventing Phishing Attacks", available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.
520 The following section describes email-based phishing attacks, compared to other phishing scams, which may, for example, be based on voice communications. See: *Gonsalves*, "Phishers Snare Victims with VoIP", 2006, available at: http://www.techweb.com/wire/security/186701001.

они могут выбрать своей целью, например финансовые институты. Правонарушители создают веб-сайты, напоминающие законные сайты "подложные сайты", где от жертвы требуется выполнить обычные процедуры входной регистрации, что позволяет правонарушителям получить личную информацию, например номера счетов и онлайновые банковские пароли.

Для того чтобы направить пользователей на подложные сайты, правонарушители отправляют по электронной почте сообщение, напоминающие сообщение электронной почты от законной компании (см. Рисунок 22)[521], что часто приводит к нарушениям торговой марки[522]. В фальшивом электронном сообщении адресатов просят войти в систему для обновления или проверки безопасности или путем угроз, например о закрытии счета, если пользователи откажутся сотрудничать. Фальшивое электронное сообщение почты обычно содержит ссылку, по которой жертва должна перейти на обманный сайт, что дает возможность избежать ввода пользователями правильного адреса своего законного банка вручную. Правонарушители разработали передовые методы, предотвращающие осознание пользователем того факта, что они находятся не на подлинном сайте[523].

Как только личная информация раскрыта, правонарушители входят в учетные записи жертв и совершают преступления, такие как перевод денежных средств, заявки на паспорта или новые счета и т. д. Рост числа успешных атак доказывает потенциал фишинга[524]. В апреле 2007 года APWG[525] сообщила о более чем 55 000 уникальных фишинг-сайтах[526]. Методы фишинга не ограничиваются только получением паролей для проведения онлайновых банковских операций. Правонарушители могут также запрашивать коды доступа к компьютерам, аукционные площадки и номера социального страхования, которые являются особенно важными в Соединенных Штатах и могут привести к преступлениям "кражи идентичности"[527].

2.9 Экономические последствия киберпреступности

Без всяких сомнений, финансовые потери, вызванные компьютерными и интернет преступлениями, существенны. Различные недавно опубликованные обзоры проанализировали экономические последствия киберпреступности[528], выдвинув на первый план их существенные последствия. Те же самые общие проблемы статистики преступности также относятся к оценкам финансовых потерь, однако сомнительно, до какой степени обзоры предоставляют точные цифры и статистические данные, поскольку многие жертвы могут не заявить о преступлениях[529].

2.9.1 Обзор результатов выбранных исследований

Институт компьютерной безопасности (ИКБ) проанализировал экономические последствия киберпреступности[530] в обзоре компьютерных преступлений и безопасности 2007 года, основанном на опросе 494 специалистов по компьютерной безопасности из корпораций США, государственных учреждений и финансовых институтов. Это имеет важное значение для Соединенных Штатов[531].

С учетом экономического цикла обзор показывает, что после роста до 2002 года, финансовые последствия киберпреступности уменьшились в течение следующих лет. Результаты обзора предполагают, что этот вывод является спорным, однако неясно, почему число зарегистрированных преступлений и средние убытки жертв

---

521 "Phishing" shows a number of similarities to spam e-mails. It is thus likely that organised crime groups that are involved in spam are also involved in phishing scams, as they make use of the same spam databases. Regarding spam, see above: Chapter 2.5.7.

522 Regarding related trademark violations, see above 2.6.2.

523 For an overview about what phishing mails and the related spoofing websites look like, see: http://www.antiphishing.org/phishing_archive/phishing_archive.html.

524 In some phishing attacks, as many as 5 per cent of victims provided sensitive information on fake websites. See *Dhamija/Tygar/Hearst*, "Why Phishing Works", available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf, page 1, that refers to *Loftesness*, "Responding to "Phishing" Attacks", Glenbrook Partners (2004).

525 Anti-Phishing Working Group. For more details, see: http://www.antiphishing.org.

526 "Phishing Activity Trends", Report for the Month of April 2007, available at: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.

527 See above: Chapter 2.7.3.

528 See, for example: "Deloitte 2007 Global Security Survey" – September 2007; "2005 FBI Computer Crime Survey"; "CSI Computer Crime and Security Survey 2007" is available at: http://www.gocsi.com/; "Symantec Internet Security Threat Report", September 2007, available at: http://www.symantec.com/enterprise/theme.jsp?themeid=threatreport; "Sophos Security Threat Report", July 2007, available at: http://www.sophos.com/pressoffice/news/articles/2007/07/securityrep.html.

529 See for example: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, 2002, page 27, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; See also ITU Study on the Financial Aspects of Network Security: Malware and Spam, July 2008, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

530 The "CSI Computer Crime and Security Survey 2007", available at: http://www.gocsi.com/

531 See "CSI Computer Crime and Security Survey 2007", page 1, available at: http://www.gocsi.com/.

возможно сократилось. В 2006 году степень убытков снова увеличилась. Обзор не объясняет уменьшения убытков в 2002 году или повышения в 2006 году. Из 21 категории, обозначенной в обзоре, самые высокие долларовые убытки были связаны с финансовым мошенничеством, вирусами, проникновением в систему извне и кражей конфиденциальных данных. Общие убытки всех опрошенных за 2006 год составили приблизительно 66,9 млн. долл. США.

После нескольких лет уменьшения средних убытков на одного опрошенного, произошел поворот событий. В 2006 г. средний убыток составил 345 000 долл. США. В 2001 году средний убыток был почти в десять раз выше (3,1 млн. долл. США). Средний убыток на одного опрошенного сильно зависит от состава опрашиваемых, если один год опрашивались, в основном, малые и средние предприятия (МСП), а в следующем году их заменили более крупные компании, то на статистические результаты сильно повлияло изменение состава опрашиваемых.

Обзор компьютерных преступлений ФБР 2005 года[532] аналогичен подходу к обзору ИКБ, но имеет более широкое освещение[533]. Обзор ФБР оценивает, что цена инцидента в системах компьютерной безопасности и интернет преступлений составила 21,7 млн. долл. США[534]. Самыми популярными преступлениями, зафиксированными организациями, стали вирусные атаки, программы-шпионы, сканирование портов и повреждение данных или сетей[535]. Обзор компьютерных преступлений ФБР 2005 года дает оценку общей сумме убытков для экономики Соединенных Штатов[536]. На основе средних убытков[537] и при условии, что компьютерными преступлениями затронуты 20% организаций США, был рассчитан общий убыток, который составил 67 млрд. долл. США[538]. Однако есть проблемы относительно того, как представить эти оценки, а также соответствие опрашиваемых год от года[539].

Доклад о вредоносном экономическом компьютерном программном обеспечении[540] 2007 года освещает последствия, оказанные на мировую экономику вредоносным программным обеспечением путем суммирования общих предполагаемых убытков[541], вызванных атаками. Одним из его ключевых результатов является тот факт, что злоумышленники, разрабатывающие вредоносные программы, переходят от вандализма к получению финансовой выгоды. В докладе говорится, что финансовые убытки, вызванные атаками вредоносных программ, достигли максимума в 2000 году (17,1 млрд. долл. США) и 2004 году (17,5 млрд. долл. США), но с 2004 года по 2006 год они уменьшились на 13,3 млрд. долл. США. Однако, как и в результатах обзора, здесь есть неопределенность относительно того, реалистичны ли статистические данные по воздействию вредоносных программ. Существуют большие несоответствия между убытками, о которых сообщают, и доказанным ущербом. Например, случай с компьютерным червем Sasser. Сообщалось о заражении миллионов компьютерных систем[542]. В ходе гражданско-правового иска против разработчика программы на просьбу присоединиться к судебному процессу, с тем чтобы доказать свои убытки, откликнулось очень немного компаний и частных лиц. Процесс закончился решением, что разработчик должен выплатить компенсацию менее десяти тысяч долларов США[543].

---

532 "2005 FBI Computer Crime Survey".

533 The 2005 FBI Computer Crime Survey is based on data of 2066 United States institutions (see 2005 FBI Computer Crime Survey, page 1) while the 2007 CSI Computer Crime and Security Survey is based on 494 respondents (See CSI Computer Crime and Security Survey 2007, page 1, available at: http://www.gocsi.com/).

534 See "2005 FBI Computer Crime Survey", page 10.

535 See "2005 FBI Computer Crime Survey", page 6.

536 See *Evers*, "Computer crimes cost $67 billion, FBI says", ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.

537 "2005 FBI Computer Crime Survey", page 10.

538 See "2005 FBI Computer Crime Survey", page 10 As well as *Evers*, "Computer crimes cost $67 billion, FBI says", ZDNet News, 19.01.2006, available at: http://news.zdnet.com/2100-1009_22-6028946.html.

539 The report makes available useful details of those institutions that responded. See "CSI Computer Crime and Security Survey 2007", page 3, available at: http://www.gocsi.com/

540 "2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code". A summary of the report is available at: http://www.computereconomics.com/article.cfm?id=1225.

541 The costs covered by the report include labour costs to analyze and repair an infected computer system, the loss of user productivity and the loss of revenue due to a loss of performance of infected computer systems. For more information, see the summary of the report available at: http://www.computereconomics.com/article.cfm?id=1225.

542 See: "Sasser Worm rips through the Internet", CNN News, 05.05.2004, available at: http://edition.cnn.com/2004/TECH/internet/05/05/sasser.worm/index.html

543 See Heise News, 06.07.2005, available at: http://www.heise.de/newsticker/meldung/print/61451.

2.9.2 Сложности, связанные со статистическими данными о киберпреступности

Неясно, насколько представительны статистические данные об экономических последствиях киберпреступности и является ли достоверной информация о степени убытков[544]. Неясно, до какой степени сообщается о киберпреступлениях не только в обзорах, но и также органам охраны правопорядка. Органы власти, участвующие в борьбе против киберпреступности, стимулируют жертв киберпреступления к сообщению об этих преступлениях[545]. Доступ к более точной информации об истинном уровне киберпреступности позволил бы органам охраны правопорядка улучшить судебное преследование злоумышленников, сдерживать потенциальные атаки и принимать более адекватные и эффективные законы.

Ряд общественных и частных организаций попытались определить количество прямых и косвенных затрат на борьбу с вредоносными программами. Сложно оценить затраты для фирм, но еще более сложно оценить финансовые убытки, причиненные вредоносными программами, и затраты отдельных клиентов, хотя есть свидетельства того, что эти убытки могут быть очень большими[546]. Однако у таких затрат есть различные компоненты. Они могут привести к прямому повреждению аппаратных средств и программного обеспечения, а так же к финансовому и другим ущербам из-за кражи идентичности или других мошеннических схем. Диапазон оценок отличается, хотя возникающая полная картина весьма последовательна.

Фирмы, с другой стороны, могут не сообщать о киберпреступлениях по нескольким причинам:

Фирмы могут опасаться, что их репутации может повредить негативная информация[547]. Если компания объявляет, что хакеры получили доступ к их серверу, клиенты могут потерять доверие. Полные затраты и последствия могли нанести больше потерь, чем потери, вызванные нападением взлома. Однако, если о злоумышленниках не сообщать и не преследовать судебным порядком, они могут продолжать нападения.

Жертвы могут не верить, что органы охраны правопорядка смогут выявить злоумышленников[548]. Сравнивая большое количество киберпреступлений с небольшим числом успешных расследований, жертвы преступлений, могут не иметь причины сообщать о преступлениях[549].

Автоматизация также означает, что киберпреступники следуют стратегии извлечения большой прибыли через множество атак на небольшие суммы, как, например, случается с мошенничеством с предоплатой[550]. Из-за очень небольших сумм жертвы могут предпочесть не проходить отнимающие много времени процедуры сообщения о преступлении. Случаи, о которых сообщается, часто основаны на чрезвычайно высоких суммах[551]. Работая только с небольшими суммами, злоумышленники разрабатывают мошенничества, которые зачастую не будут расследоваться в дальнейшем.

---

544 Regarding the related difficulties see: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 229, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

545 "The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office". See Heise News, 27.10.2007, available at: http://www.heise-security.co.uk/news/80152.

546 ITU Study on the Financial Aspects of Network Security: Malware and Spam, July 2008, available at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf.

547 See *Mitchison/Urry*, "Crime and Abuse in e-Business, IPTS Report", available at: http://www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm

548 See Smith, "Investigating Cybercrime: Barriers and Solutions", 2003, page 2, available at: http://www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf

549 In fact, newspapers as well as TV stations limit their coverage of successful Internet investigations to spectacular cases such as the identification of a paedophile by descrambling manipulated pictures of the suspect. For more information about the case and the coverage, see: "Interpol in Appeal to find Paedophile Suspect", The New York Times, 09.10.2007, available at: http://www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: http://www.interpol.int/Public/THB/vico/Default.asp.

550 See SOCA, "International crackdown on mass marketing fraud revealed, 2007", available at: http://www.soca.gov.uk/downloads/massMarketingFraud.pdf.

551 In the 2006 NW3C Internet Crime report, only 1.7 per cent of the reported total USD losses were related to the Nigerian Letter Fraud, but those cases that were reported had an average loss of 5,100 USD each. The number of reported offences is very low, while the average loss of those offences is the high.

3 ПРОБЛЕМЫ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Последние разработки в области ИКТ не только привели к новым преступлениями и новым методам совершения преступлений, но и новым методам расследования киберпреступлений. Достижения в области ИКТ значительно расширили возможности органов охраны правопорядка. И наоборот, преступники могут использовать новые средства, для того чтобы воспрепятствовать идентификации и затруднить расследование. В этой главе основное внимание уделяется проблемам борьбы с киберпреступностью.

3.1 Благоприятные возможности

Органы охраны правопорядка теперь могут использовать для судебной экспертизы компьютерные системы повышенной производительности и сложные программы для ускорения расследования и автоматизации процедур поиска[552].

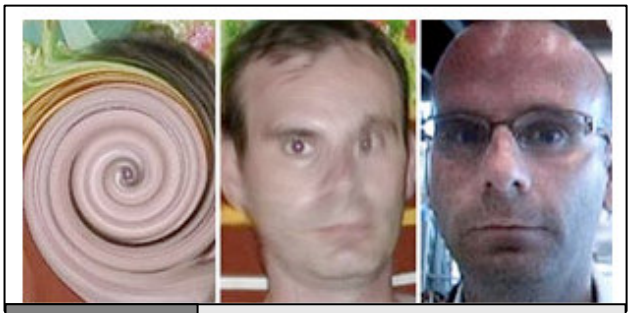


Рисунок 23

В примере, приведенном выше, компьютерные судебные эксперты смогли разложить внесенные в фотографию изменения и реконструировать лицо подозреваемого.

Это может затруднить автоматизацию процессов расследования. Хотя поиск незаконного содержания по ключевым словам может быть легко осуществлен, идентификация незаконных изображений является более проблематичной. Подходы на основе значений хэш-функции успешны только, если изображения были предварительно обсчитаны, значение хэш-функции хранится в базе данных и проанализированное изображение не было изменено[553].

Программы для судебной экспертизы способны автоматически искать изображения детской порнографии, сравнивая файлы на жестком диске подозреваемого с информацией об известных изображениях. Например, в конце 2007 года, власти нашли несколько изображений сексуального насилия над детьми. Для предотвращения идентификации преступник цифровым способом изменил часть изображений, показывающих его лицо, перед публикацией изображений в интернет (см. Рисунок 23). Компьютерные судебные эксперты смогли разложить изменения и реконструировать лицо подозреваемого[554]. Хотя успешное расследование явно демонстрирует возможности компьютерной судебной экспертизы, этот случай не является доказательством прорыва в расследования детской порнографии. Если бы преступник просто закрыл свое лицо белым пятном, идентификация была бы невозможна.

---

[552] See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf; *Reith*, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

[553] Regarding hash-value based searches for illegal content see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 546 et seq.; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

[554] For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: http://www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: http://www.interpol.int/Public/THB/vico/Default.asp

3.2 *Общие проблемы*

3.2.1 Зависимость от ИКТ

Многие виды повседневной связи зависят от ИКТ и услуг, связанных с интернетом, включая вызовы VoIP или сообщения электронной почты[555]. ИКТ в настоящее время отвечает за контроль и управление функциями в зданиях[556], автомобилях и авиационных службах (см. Рисунок 24[557]). Энергоснабжение, водоснабжение и услуги связи зависят от ИКТ. В дальнейшем интеграция ИКТ в повседневную жизнь, скорее всего, продолжится[558].

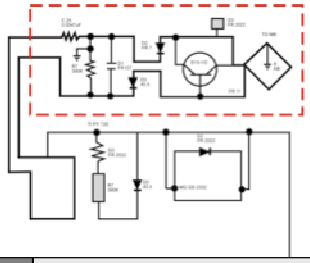


Рисунок 24

Информационные технологии и электронные устройства все больше заменяют функции ручного управления.

Растущая зависимость от ИКТ делает системы и услуги более уязвимыми для атак на важнейшие инфраструктуры[559]. Даже короткие перерывы в предоставлении услуг могут привести к огромным финансовым потерям для предприятия электронной коммерции[560], не только гражданская связь может быть прервана атаками; зависимость от ИКТ является основным риском для военной связи[561].

Существующая техническая инфраструктура имеет ряд слабых мест, таких как монокультуры или однородность операционных систем. Многие частные пользователи, а также малые и средние предприятия используют операционную систему Microsoft[562], таким образом преступники могут разрабатывать эффективные атаки, концентрируя внимание на этой единственной цели[563].

Зависимость общества от ИКТ не ограничивается западными странами[564] – развивающиеся страны также сталкиваются с проблемами в предотвращении атак на свои инфраструктуры и пользователей[565]. Развитие более

---

555 It was reported that the United States Department of Defence had to shut down their e-mail system after a hacking attack. See: http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

556 Examples include the control of air-conditioning, access and surveillance systems, as well as the control of elevators and doors.

557 See *Goodman*, "The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

558 *Bohn/Coroama/Langheinrich/Mattern/Rohs,* "Living in a World of Smart Everyday Objects – Social, Economic & Ethical Implications", Journal of Human and Ecological Risk Assessment, Vol. 10, page 763 et seqq., available at: http://www.vs.inf.ethz.ch/res/papers/hera.pdf.

559 Re the impact of attacks, see: *Sofaer/Goodman*, "Cybercrime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf.

560 A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm, 'sasser". In 2004, the computer worm affected computers running versions of Microsoft's operation System Windows. As a result of the worm, a number of services were interrupted. Among them were the U.S. airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: http://www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

561 *Shimeall/Williams/Dunlevy*," Countering cyber war", NATO review, Winter 2001/2002, page 16, available at: http://www.cert.org/archive/pdf/counter_cyberwar.pdf.

562 One analysis by "Red Sheriff" in 2002 stated that more than 90% of the users worldwide use Microsoft`s operating systems (source: http://www.tecchannel.de - 20.09.2002).

563 Re the discussion about the effect of the monoculture of operating systems on cybersecurity, see *Picker*, "Cyber Security: Of Heterogeneity and Autarky", available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf; "Warning: Microsoft 'Monoculture'", Associated Press, 15.02.2004, available at http://www.wired.com/news/privacy/0,1848,62307,00.html; *Geer and others*, "CyberInsecurity: The Cost of Monopoly", available at: http://cryptome.org/cyberinsecurity.htm.

564 With regards to the effect of spam on developing countries, see: "Spam issues in developing countries, 2005", available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

565 Regarding the integration of developing countries in the protection of network infrastructure, see: "Chairman's Report on ITU Workshop On creating trust in Critical Network Infrastructures", available at: http://www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; "World Information Society Report 2007", page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

дешевых технологий инфраструктуры, таких как WiMAX[566], позволяет развивающимся странам предлагать услуги интернет большему числу людей. Развивающиеся страны могут избежать ошибок некоторых западных стран, которые в основном сосредоточены на максимизации доступности, без значительного инвестирования в защиту. Эксперты США пояснили, что успешные атаки на официальный сайт государственных организаций в Эстонии[567] мог иметь место только в связи с неадекватностью мер защиты[568]. Развивающиеся страны обладают уникальной возможностью для интеграции мер по обеспечению безопасности на ранней стадии. Это может потребовать больших авансовых инвестиций, но интеграция мер по обеспечению безопасности на более позднем этапе может оказаться более дорогостоящей в долгосрочном плане[569].

Должны быть разработаны стратегии для предотвращения таких атак и разработаны контрмеры, включающие в себя разработку и продвижение технических средств защиты, а также адекватных и обоснованных законов, позволяющих правоохранительным органам эффективно бороться с киберпреступностью[570].

3.2.2 Количество пользователей

Популярность интернета и его услуг стремительно растет, в мире насчитывается более 1 млрд. пользователей интернета (см. Рисунок 25[571]). Компьютерные компании и поставщики услуг интернет сосредоточены на развивающихся странах с большим потенциалом для дальнейшего роста[572]. В 2005 году число пользователей интернета в развивающихся странах превысило их число в промышленно-развитых странах[573], в то время как развитие дешевых аппаратных средств и беспроводной доступ позволит получить доступ к интернету еще большему числу людей[574].

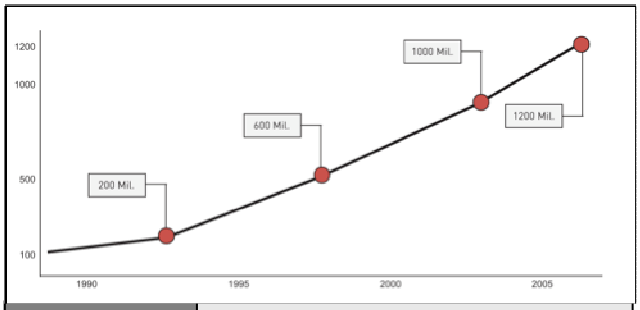


Рисунок 25

В настоящее время более насчитывается более 1 миллиарда пользователей интернета.

С ростом числа людей, подключенных к интернету, количество целей и преступников возрастает[575]. Сложно оценить, сколько людей используют интернет для незаконной деятельности. Даже если лишь 0,1% пользователей совершили преступления, общее количество правонарушителей было бы более миллиона. Хотя в развивающихся странах степень использования интернета ниже, содействие кибербезопасности не легче, поскольку преступники могут совершать преступления из любой точки всего мира[576].

Увеличение числа пользователей интернета вызывает трудности для органов охраны правопорядка, поскольку оно довольно серьезно затрудняет автоматизацию процессов расследования. Хотя поиск незаконных материалов по ключевому слову может быть легко проведен, идентификация незаконного

---

566 WiMAX (Worldwide Interoperability for Microwave Access) is a technology that provides wireless data services over long distances. For more information, see: The WiMAX Forum, available at http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, "WiMAX Technology for Broadband Wireless Access".

567 Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: http://www.cert.hu/dmdocuments/Estonia_attack2.pdf

568 See: *Waterman*: Analysis: Who cyber smacked Estonia, United Press International 2007, available at: http://www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

569 Regarding cybersecurity in developing countries see: World Information Society Report 2007, page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

570 See below: Chapter 4.

571 According to the ITU, there were 1.14 billion Internet users by the start of 2007, available at: http://www.itu.int/ITU-D/icteye.default.asp.

572 See *Wallsten*, "Regulation and Internet Use in Developing Countries", 2002, page 2.

573 See "Development Gateway's Special Report, Information Society – Next Steps?", 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

574 An example for new technology in this area is WiMAX (Worldwide Interoperability for Microwave Access), a standards-based wireless technology that provides broadband connections over long distances. Each WiMAX node could enable high-speed Internet connectivity in a radius of up to 50 km. For more information, see: The WiMAX Forum at http://www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

575 Regarding the necessary steps to improve cybersecurity, see: "World Information Society Report 2007", page 95, available at: http://www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

576 The fact that the offenders are not only based in western countries is proven by current analysis that suggests for example that an increasing number of phishing websites are hosted in developing countries. For more details, see: "Phishing Activity Trends", Report for the Month of April 2007, available at: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: Chapter 2.8.d.

изображения является более проблематичной. Подходы на основе значений хэш-функции, успешны только, если изображения были предварительно обсчитаны, значение хэш-функции хранится в базе данных и проанализированное изображение не было изменено[577].

3.2.3 Наличие устройств и доступа

Только базовое оборудование, необходимое для совершения компьютерных преступлений, обычно включает следующие элементы:

- аппаратные средства;
- программное обеспечение; и
- доступ в интернет.

Что касается аппаратных средств, производительность компьютеров непрерывно растет[578]. Есть целый ряд проектов, позволяющих людям в развивающихся странах использовать ИКТ более широко[579]. Преступники могут совершать тяжкие компьютерные преступления, используя дешевую или подержанную компьютерную технику, они гораздо больше рассчитывают на знания, чем оборудование. Версия компьютерной технологии практически не влияет на использование этого оборудования с целью совершения преступления.

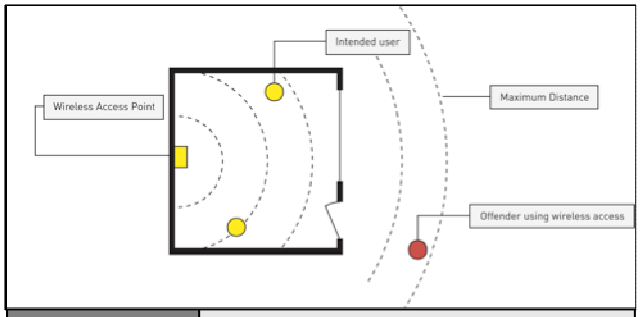


Рисунок 26

Доступ к интернету, не оставляя следов, является первоочередной задачей для многих преступников. На рисунке показано, как правонарушитель может использовать сигнал открытой беспроводной сети для получения удаленного доступа. В таких случаях практически невозможно идентифицировать преступника.

Совершение киберпреступлений может быть упрощено средствами специализированного программного обеспечения. Правонарушители могут загрузить программы[580], предназначенные для обнаружения открытых портов или взлома парольной защиты[581]. Широкую доступность таких устройств трудно ограничить из-за применения методов зеркалирования и одноранговой коммутации[582].

Последнее является жизненно важным элементом доступа в интернет. Несмотря на то, что в большинстве развивающихся стран стоимость доступа в интернет[583] выше, чем в промышленных странах, число пользователей интернета в развивающихся странах растет быстрыми темпами[584]. Правонарушители, как правило, не подписываются на услуги интернета, чтобы снизить возможность обнаружения, но предпочитают услуги, которыми они могут пользоваться без (проверяемой) регистрации. Типичным способом получения доступа к сети является так называемый "wardriving". Этот термин описывает передвижение в поиске доступных беспроводных сетей[585]. Наиболее распространенными способами доступа правонарушителей к сетевым соединениям являются:

- терминалы интернета общего пользования;

---

577 Regarding hash-value based searches see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

578 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law). For more information. see *Moore*, "Cramming more components onto integrated circuits", Electronics, Volume 38, Number 8, 1965, available at: ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf; *Stokes*, "Understanding Moore's Law", available at: http://arstechnica.com/articles/paedia/cpu/moore.ars/.

579 Chapter six, "World Information Society Report 2007", ITU, Geneva, available at: http://www.itu.int/wisr/

580 "Websense Security Trends Report 2004", page 11, available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; "Information Security - Computer Controls over Key Treasury Internet Payment System", GAO 2003, page 3, available at: http://www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

581 *Ealy*, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", page 9 et seqq., available at: http://www.212cafe.com/download/e-book/A.pdf.

582 In order to limit the availability of such tools, some countries criminalise the production and offer of such tools. An example of such a provision can be found in Art. 6 of the European Convention on Cybercrime. See below: Chapter 6.1.13.

583 Regarding the costs, see: The World Information Society Report, 2007, available at: http://www.itu.int/wisr/

584 See "Development Gateway's Special Report, Information Society – Next Steps?", 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

585 For more information see: *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: http://www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf

- открытые беспроводные сети (см. Рисунок 26[586]);
- взломанные сети; и
- услуги с предоплатой без регистрации.

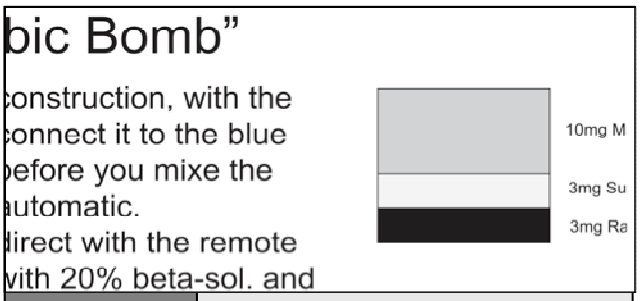


Рисунок 27

В интернете широко представлены инструкции о том, как сделать оружие и взрывчатые вещества. На рисунке показаны объяснения, как сделать бомбу только с помощью доступных в аптеках компонентов.

Органы охраны правопорядка принимают меры по ограничению неконтролируемого доступа к услугам интернет во избежание преступного злоупотребления этими услугами. В Италии и Китае, например использование терминалов интернет общего пользования требует идентификации пользователей[587]. Однако существуют аргументы против подобных требований идентификации[588]. Несмотря на то, что ограничение доступа может предотвратить преступления и облегчить расследования, проводимые органам охраны правопорядка, такое законодательство может препятствовать росту информационного общества и развитию электронной коммерции[589]. Было высказано мнение, что такое ограничение на доступ в интернет может нарушать права человека[590]. Например, Европейский суд в ряде случаев вынес решения в отношении вещания, что право на свободное выражение относится не только к содержанию информации, но и к средствам передачи или приема. В деле Autronic против Швейцарии[591], суд постановил, что расширенное толкование необходимо, поскольку любые ограничения, введенные в отношении средств передачи, неизбежно нарушают право получать и распространять информацию. Если эти принципы применяются для потенциальных ограничений доступа в интернет, возможно, что такие законодательные подходы могут повлечь за собой нарушение прав человека.

3.2.4 Доступность информации

Интернет содержит миллионы веб-страниц[592] новейшей информации. Принять участие может каждый, кто публикует и поддерживает веб-страницы. Одним из примеров успеха платформ, создаваемых пользователями, является Википедия[593] – онлайновая энциклопедия, где каждый может опубликовать свой материал[594].

Успех в интернете также зависит от мощных поисковых систем, которые позволяют пользователям искать по миллионам веб-страниц в секунду. Эта технология может быть использована как в законных, так и в преступных целях. Термин "Googlehacking" или "Googledorks" описывает использование комплексных запросов поисковых систем для фильтрации результатов поиска информации о компьютерной безопасности.

---

586 With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: “The Wireless Internet Opportunity for Developing Countries, 2003”, available at: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

587 One example of an approach to restrict the use of public terminals for criminal offences is Art. 7 of the Italian Decree-Law No. 144. Decree-Law 27 July 2005, no. 144 – “Urgent measures for combating international terrorism”. For more information about the Decree-Law, see for example the article “Privacy and data retention policies in selected countries”, available at http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

588 See below: Chapter 6.2.11.

589 Regarding the impact of censorship and control, see: *Burnheim*, “The right to communicate, The Internet in Africa”, 1999, available at: http://www.article19.org/pdfs/publications/africa-internet.pdf

590 Regarding the question whether access to the Internet is a human right, see: *Hick/Halpin/Hoskins*, “Human Rights and the Internet”, 2000; Regarding the declaration of Internet Access as a human right in Estonia, see: “Information and Communications Technology”, in UNDP Annual Report 2001, Page 12, available at: http://www.undp.org/dpa/annualreport2001/arinfocom.pdf; “Background Paper on Freedom of Expression and Internet Regulation”, 2001, available at: http://www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

591 Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47. Summary available at: http://sim.law.uu.nl/sim/caselaw/Hof.nsf/2422ec00f1ace923c1256681002b47f1/cd1bcbf61104580ec1256640004c1d0b?OpenDocument.

592 The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: http://www.isc.org/index.pl?/ops/ds/reports/2007-07/; The Internet monitoring company Netcraft reported in August 2007 a total of nearly 130 million websites at: http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html.

593 http://www.wikipedia.org

594 In the future development of the Internet, information provided by users will become even more important. “User generated content” is a key trend among the latest developments shaping the Internet. For more information, see*: O’Reilly*, “What Is Web 2.0 - Design Patterns and Business Models for the Next Generation of Software”, 2005, available at: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

Например, правонарушители могут искать незащищенные системы парольной защиты[595]. Отчеты подчеркивают риск использования поисковых систем в незаконных целях[596]. Правонарушитель, планирующий нападение, может найти в интернете подробную информацию, объясняющую, как сделать бомбу с использованием только тех химических веществ, которые продаются в обычных супермаркетах (Рисунок 27[597]). Несмотря на то, что эта информация была доступна даже до появления интернет, однако получить доступ к этой информации было намного труднее. Сегодня получить доступ к этим инструкциям может любой пользователь интернета.

Преступники могут также использовать поисковые системы для анализа целей нападения[598]. В ходе расследования в отношении членов одной террористической группы было найдено учебное пособие, подчеркнувшее, насколько полезен интернет для сбора информации о возможных целях нападения[599]. С помощью поисковых систем правонарушители могут собирать общедоступную информацию, например строительные планы общественных зданий, помогающую в их подготовке. Сообщалось, что повстанцы, совершившие нападения на британские войска в Афганистане, использовали спутниковые снимки из Google Earth[600].

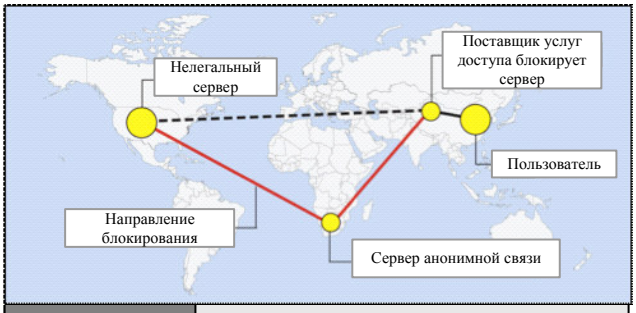


Рисунок 28

На рисунке показана возможность обойти механизмы централизованного контроля, установленные поставщиками услуг доступа. Если доступ к оферентов установки некоторых фильтров технологий, запросы пользователей будут блокироваться. Этот подход контроля может быть обойден, если пользователь использует серверы анонимной связи, шифрующие запросов. Например, в этом случае поставщики услуг доступа не имеют доступа к запросам, направленным на сервер анонимной связи, и не может блокировать веб-сайты.

3.2.5 Нехватка механизмов контроля

Для обеспечения работоспособности всех сетей массовых коммуникаций: от телефонной сети, используемой для голосовых телефонных звонков, до интернета, – требуются централизованное управление и технические стандарты. Продолжающиеся дискуссии об управлении интернетом полагают, что интернет не имеет отличий по сравнению с национальной или даже и транснациональной инфраструктурой связи[601]. Кроме того, необходимо законодательное регулирование интернета, и законодатели вместе с органами охраны правопорядка приступили к разработке правовых норм, устанавливающих определенную степень централизованного контроля.

Интернет изначально был разработан как военная сеть[602], построенная по децентрализованной сетевой архитектуре, которая должна сохранять неизменными и действующими свои основные функции, даже если компоненты сети были атакованы. В результате инфраструктура сети интернет устойчива к внешним попыткам управления. Он изначально не был предназначен для облегчения уголовного расследования или предотвращения атак внутри сети.

---

595 For more information, see: *Long/Skoudis/van Eijkelenborg*, "Google Hacking for Penetration Testers, 2005"; *Dornfest/Bausch/Calishain*, "Google Hacks: Tips & Tools for Finding and Using the World's Information", 2006.

596 See Nogguchi, 'search engines lift cover of privacy", The Washington Post, 09.02.2004, available at: http://www.msnbc.msn.com/id/4217665/print/1/displaymode/1098/.

597 One example is the "Terrorist Handbook" – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

598 See *Thomas*, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", Parameters 2003, page 112 et seqq., available at: http://www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf; *Brown/Carlyle/Salmerón/Wood*, "Defending Critical Infrastructure", Interfaces, Vol. 36, No. 6, page 530, available at: http://www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.

599 "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy". The reports about the sources of the quotation varies: The British High Commissioner Paul Boateng mentioned in a speech in 2007 that the quote was "contained in the Al Qaeda training manual that was recovered from a safe house in Manchester" (see: Boateng, "The role of the media in multicultural and multifaith societies", 2007, available at: http://www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1125560437610&a=KArticle&aid=1171452755624. The United States Department of Defence reported that the quote was taken from an Al Qaeda Training Manual recovered in Afghanistan (see: http://www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html). Regarding the availability of sensitive information on websites, see: *Knezo*, "Sensitive but Unclassified" Information and Other Controls: Policy & Options for Scientific and Technical Information, 2006, page 24, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-8704:1.

600 See Telegraph.co.uk, news from January the 13th 2007.

601 See for example, *Sadowsky/Zambrano/Dandjinou*, "Internet Governance: A Discussion Document", 2004, available at: http://www.internetpolicy.net/governance/20040315paper.pdf;

602 For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; lynch, Postel, Roberts, Wolff*, "A Brief History of the Internet", available at: http://www.isoc.org/internet/history/brief.shtml.

Сегодня интернет все шире используется для гражданских служб. При переходе от военной к гражданской службе сущность требований к инструментам управления не изменилась. Поскольку сеть основана на протоколах, разработанных для военных целей, инструменты централизованного управления отсутствуют, и их нельзя ввести, без существенного изменения конфигурации сети. Отсутствие инструментов контроля делает расследование киберпреступлений весьма затруднительным[603].

Одним из примеров проблем, возникающих из-за отсутствия инструментов управления является способность пользователей обходить технологию фильтрации[604], используя услуги кодированной анонимной связи[605]. Если поставщик услуг доступа блокирует доступ к определенным веб-сайтам с незаконным содержанием, например с детской порнографией, то потребители, как правило, не могут получить доступ к этим веб-сайтам. Но блокирование незаконного содержания можно обойти, если потребители используют серверы анонимной связи, шифрующие сообщения между ними и центральным сервером. В этом случае поставщики услуг могут оказаться не в состоянии блокировать запросы, поскольку запросы направляются в виде зашифрованных сообщений, которые не могут быть открыты поставщиками услуг доступ (Рисунок 28).

3.2.6 Международные масштабы

Многие процессы передачи данных затрагивают более одной страны[606]. Протоколы, используемые для передачи данных в интернете, основаны на оптимальной маршрутизации, если прямые линии временно заблокированы[607]. Даже тогда, когда внутренние процессы передачи в пределах страны происхождения ограничены, данные могут покинуть страну, они передаются через маршрутизаторы, находящиеся за пределами данной территории, и перенаправляются обратно в страну конечного назначения[608]. Кроме того, многие услуги интернета основаны на зарубежных услугах[609], например поставщики услуг хостинга могут предложить арендовать веб-пространство в одной стране, имея аппаратные средства в другой стране[610].

---

603 *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

604 Regarding filter obligations/approaches see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. Seq., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion about filtering in different countries see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: http://www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: http://www.ip-watch.org/weblog/index.php?p=842; Zwenne, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement , available at: http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf; Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf.

605 For more information regarding anonymous communications, see below: Chapter 3.2.l2.

606 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

607 The first and still most important communication protocols are: Transmission Control Protocol (TCP) and Internet Protocol (IP). For further information, see: *Tanebaum*, Computer Networks; *Comer*, "Internetworking with TCP/IP – Principles, Protocols and Architecture".

608 See *Kahn/Lukasik*, "Fighting Cyber Crime and Terrorism: The Role of Technology," presentation at the Stanford Conference, December 1999, page 6 et seqq.; *Sofaer/Goodman*," Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 6, available at: http://media.hoover.org/documents/0817999825_1.pdf.

609 One example of the international cooperation of companies and the delegation within international companies is the Compuserve case. The head of the German daughter company (Compuserve Germany) was prosecuted for making child pornography available that was accessible through the computer system mother company in the United States connected to the German company. See *Amtsgericht Muenchen*, Multimedia und Recht 1998, Page 429 et seq. (with notes *Sieber).*

610 See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplyfing Data Storage and Management.

Если правонарушители и цели нападения находятся в разных странах, то для расследования киберпреступлений необходимо сотрудничество органов охраны правопорядка всех затронутых стран[611]. Национальный суверенитет не допускает расследования на территории разных стран без разрешения местных властей[612]. Расследования киберпреступлений нуждаются в поддержке и участии органов власти всех затронутых стран.

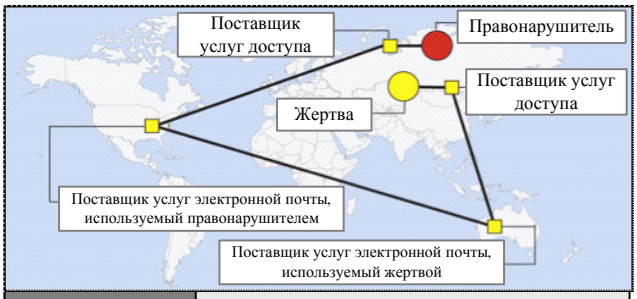


Рисунок 29

На рисунке показано, что даже если правонарушители и цели расположены в одной стране, процесс передачи по электронной почте незаконного содержания может проходить и пересекать различные страны. Иначе, процесс передачи данных может быть направлен за пределы страны, а затем перенаправлен обратно.

Трудно строить сотрудничество в области киберпреступности на традиционных принципах взаимной правовой помощи. Формальные требования и время, необходимое для сотрудничества с иностранными органами охраны правопорядка, зачастую затрудняют расследование[613]. Расследования часто выполняются в сжатые сроки[614]. Данные, имеющие большое значение для отслеживания преступлений, зачастую очень быстро удаляются. Сжатые сроки расследования вносят проблемы, поскольку для организации традиционного режима взаимной правовой помощи зачастую требуется много времени[615]. Принцип обоюдного признания деяния преступлением[616] также создает трудности, если в одной из стран, участвующих в расследовании, данное правонарушение не квалифицируется как преступление[617]. Правонарушители могут сознательно использовать в своих атаках третьи страны, с тем чтобы затруднить расследование[618].

Преступники могут сознательно выбирать цели нападения за пределами своей страны и действовать в странах с недостаточно строгим законодательством в сфере киберпреступности (Рисунок 29)[619]. Возможно, определенную помощь здесь окажут гармонизация законодательства в сфере киберпреступности и международное сотрудничество. Двумя подходами к ускорению международного сотрудничества в расследовании киберпреступлений являются G8 сеть 24/7[620] и положения, касающиеся международного сотрудничества, содержащиеся в Конвенции Совета Европы о киберпреступности[621].

---

611 Regarding the need for international cooperation in the fight against Cybercrime, see: *Putnam/Elliott,* "International Responses to Cyber Crime", in Sofaer/Goodman, " Transnational Dimension of Cyber Crime and Terrorism", 2001, page 35 et seqq., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 1 et seqq., available at: http://media.hoover.org/documents/0817999825_1.pdf

612 National Sovereignty is a fundamental principle in International Law. See *Roth*, 'state Sovereignty, International Legality, and Moral Disagreement", 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

613 See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf;

614 See below: Chapter 3.2.10.

615 See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142.

616 Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

617 Regarding the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf.

618 See: *Lewis*, "Computer Espionage, Titan Rain and China", page 1, available at: http://www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

619 Regarding the extend of cross-border cases related to Computer Fraud see: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 9, available at: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

620 See below: Chapter 6.3.8.

621 See below: Chapter 6.3.

3.2.7 Независимость от местоположения и присутствия на месте преступления

Преступникам не обязательно находиться в том же месте, где находится цель нападения. Так как местоположение преступника может полностью отличаться от места преступления, множество киберпреступлений являются транснациональными. Международные киберпреступления требуют затрат времени и усилий. Киберпреступники стараются избегать стран с развитым законодательством в отношении киберпреступлений (Рисунок 30[622]).

Предотвращение создания "безопасных гаваней" является одной из главных задач борьбы с киберпреступностью[623]. Пока существуют "безопасные гавани" злоумышленники будут использовать их для создания препятствий следствию. Развивающиеся страны, которые еще не приняли законодательства по киберпреступности, могут быть уязвимыми, так как преступники могут выбрать эти страны для своих баз, чтобы избегать наказаний. Тяжкие преступления, жертвы которых расположены по всему миру, трудно остановить, если в странах, где находятся злоумышленники, нет адекватного законодательства. Это может привести к оказанию на определенные страны давления, побуждающего принять такие законы. Одним из примеров такой ситуации является компьютерный червь "Love Bug", созданный тем, кто подозревается в этом преступлении, на Филиппинах в 2000 году[624], этот червь заразил миллионы компьютеров по всему миру[625]. Расследование на местном уровне было затруднено тем, что на тот момент на Филиппинах создание и распространение вредоносных программ не преследовалось судебным порядком должным образом[626]. Другим примером служит Нигерия, которая испытывает на себе давление в отношении принятия мер к финансовых аферам, распространяемых по электронной почте.

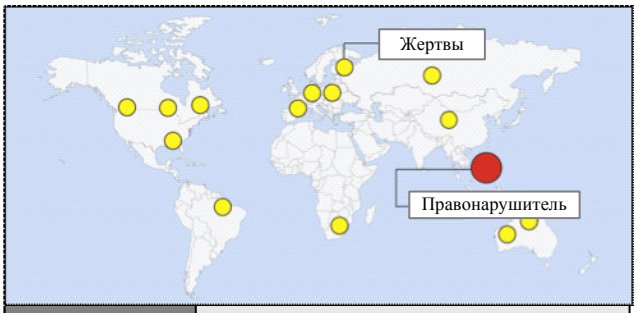


Рисунок 30

Злоумышленники могут использовать интернет для совершения преступлений практически из любой точки Земного шара. Задачи, которые возможные злоумышленники учитывают, решая, где им создать свою базу, включают в себя: состояние законодательства по киберпреступности, эффективность органов охраны правопорядка и доступность анонимного доступа в интернет.

3.2.8 Автоматизация

Одним из главных преимуществ ИКТ является возможность автоматизации определенных процессов. Автоматизация имеет несколько основных последствий:

- Она ускоряет процессы;
- Она увеличивает масштабы и влияние процессов;
- Она ограничивает участие людей.

---

622 One example is phishing. Although most sites are still stored in the United States (32%), which has strong legislation in place, countries such as China (13%), Russia (7%) and the Republic of Korea (6%), which may have less effective instruments in the field of international cooperation in place, are playing a more important role. Apart from the United States, none of them has yet signed and ratified cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

623 This issue was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: Chapter 5.2.

624 For more information, see http://en.wikipedia.org/wiki/ILOVEYOU; regarding the effect of the worm on Critical Information Infrastructure Protection, see: *Brock*, "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000, available at: http://www.gao.gov/archive/2000/ai00181t.pdf.

625 BBC News, "Police close in on Love Bug culprit", 06.05.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/738537.stm. Regarding the technology used, see: http://radsoft.net/news/roundups/luv/20000504,00.html.

626 See for example: CNN, "Love Bug virus raises spectre of cyberterrorism", 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, "A Critical Look at the Regulation of Cybercrime", http://www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

Автоматизация уменьшает потребность в дорогостоящей рабочей силе, позволяя поставщикам предлагать услуги по низким ценам[627]. Злоумышленники могут использовать автоматизацию для увеличения масштабов своей деятельности, многомиллионный вал нежелательных спамовых сообщений[628] можно разослать автоматически[629] (см. Рисунок 31). В настоящее время зачастую автоматизированы также и хакерские атаки[630], и ежедневно насчитывается 80 миллионов хакерских атак[631], что стало возможным благодаря использованию программных инструментов[632], способных атаковать тысячи компьютерных систем за несколько часов[633]. Благодаря автоматическим процессам, злоумышленники могут получать большие преимущества, осуществляя аферы, с большим количеством преступлений и относительно небольшими потерями каждой жертвы[634]. Чем ниже отдельные потери, тем выше шанс того, что жертва не сообщит о преступлении.

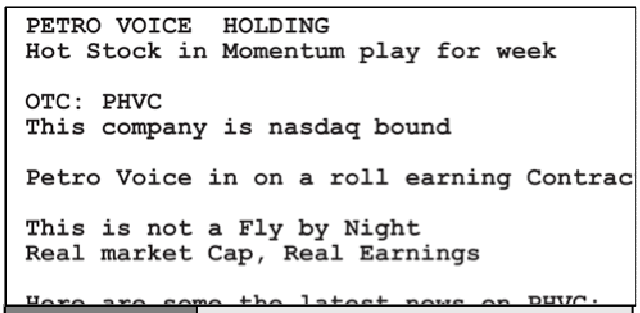


Рисунок 31

Одним из примеров процессов автоматизации является распространение спама. За небольшой период времени можно разослать миллионы электронных писем.

Автоматизация атак особенно затрагивает развивающиеся страны. Из-за ограниченных ресурсов развивающихся стран спам для них может стать намного большей угрозой, чем для промышленно-развитых стран[635]. Это большее число преступлений, которые могут быть совершены при помощи автоматизации, ставит сложные задачи перед органами охраны правопорядка по всему миру, так как они должны быть готовы к росту числа жертв в рамках своей юрисдикции.

3.2.9 Ресурсы

Современные компьютерные системы, появляющиеся в настоящее время на рынке, являются очень высоко производительными и могут применяться для расширения преступной деятельности. Но проблемы для расследования создает не только растущая производительность[636] компьютеров отдельных пользователей. Увеличивающиеся возможности сетей также представляют собой большую проблему.

Одним из примеров служат недавние атаки на правительственные сайты Эстонии[637]. Анализ атак позволяет предположить, что они совершались с нескольких тысяч компьютеров, образующих сетевого робота[638], или группы взломанных компьютеров, на которых работали программы, управляемые извне[639]. В большинстве случаев компьютеры заражены вредоносным программным обеспечением, устанавливающим инструменты,

---

627 One example of low- cost services that are automated is e-mail. The automation of registration allows providers offer e-mail addresses free of charge. For more information on the difficulties of prosecuting Cybercrime involving e-mail addresses, see below: Chapter 3.2.l.

628 The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: "ITU Survey on Anti-Spam Legislation Worldwide 2005", page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

629 For more details on the automation of spam mails and the challenges for law enforcement agencies, see: *Berg*, "The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies", Michigan Law Journal 2007, page 21, available at: http://www.michbar.org/journal/pdf/pdf4article1163.pdf.

630 *Ealy*, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", page 9 et seqq., available at: http://www.212cafe.com/download/e-book/A.pdf.

631 The Online-Community HackerWatch publishes regular reports on hacking attacks. Based on their sources, more than 250 million incidents were reported in only one month (August 2007). Source: http://www.hackerwatch.org.

632 Regarding the distribution of hacking tools, see: CC Cert, "Overview of Attack Trends", 2002, page 1, available at: http://www.cert.org/archive/pdf/attack_trends.pdf.

633 See CC Cert, "Overview of Attack Trends", 2002, page 1, available at: http://www.cert.org/archive/pdf/attack_trends.pdf.

634 Nearly 50% of all fraud complains reported to the United States Federal Trade Commission are related to a amount paid between 0 and 25 USD. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission , available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

635 See 'spam Issue in Developing Countries", Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf

636 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).

637 Regarding the attacks, see: Lewis, "Cyber Attacks Explained", 2007, available at: http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; "A cyber-riot", The Economist, 10.05.2007, available at: http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; "Digital Fears Emerge After Data Siege in Estonia", The New York Times, 29.05.2007, available at: http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

638 See: *Toth*, "Estonia under cyber attack", http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

639 See: *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime", 2005, page 3, available at: http://www.cert.org/archive/pdf/Botnets.pdf;

позволяющие преступникам захватывать управление (см. Рисунок 32). Сетевые роботы используются для сбора информации о целях нападений или для высокоуровневых атак[640].

За последнее время сетевые роботы стали серьезной угрозой кибербезопасности[641]. Размеры сетевых роботов могут составлять от нескольких до более миллиона компьютеров[642]. Современный анализ указывает на то, что примерно четверть всех компьютеров, соединенных с интернетом, может быть заражена программами, делающих их частью сетевого робота[643]. Сетевые роботы могут использоваться для различных преступных действий, включая:

- атаки типа "Отказ в обслуживании[644]";
- рассылку спама[645];
- хакерские атаки; и
- файлообменные сети.

Рисунок 32

Два рисунка выше показывают процесс создания и использования сетевого робота.

Сетевые роботы дают злоумышленникам ряд преимуществ. Они облегчают преступникам проникновение в компьютеры и в сети. При помощи тысяч компьютерных систем преступники могут атаковать другие компьютерные системы, которые будут в пределах досягаемости, причем физически используя для атаки несколько компьютеров[646]. Сетевые роботы также затрудняют возможность отследить первоначального злоумышленника, так как начальные следы приведут только к участнику сетевого робота. Так как преступники контролируют все больше мощных компьютерных систем и сетей, разрыв между возможностями следственных органов и систем, управляемых преступниками, постоянно растет.

3.2.10 Скорость процессов обмена данными

Передача электронных писем между странами занимает всего лишь несколько секунд. Такой короткий промежуток времени является одной из причин успеха интернета, так как электронные письма исключили затраты времени на физическую доставку сообщений. Однако такая быстрая передача оставляет органам охраны правопорядка мало времени для проведения расследований или сбора доказательств. Обычные расследования длятся намного дольше[647].

Одним из примеров является передача детской порнографии. В прошлом видеоматериалы вручались или доставлялись покупателям. И передача, и доставка давали органам охраны правопорядка возможность расследования. Основным различием между обменом детской порнографией через интернет и без использования интернета является транспортировка. Когда злоумышленник использует интернет, обмен фильмами можно произвести за секунды.

---

640 See: *Ianelli/Hackworth*, "Botnets as a Vehicle for Online Crime", 2005, available at: http://www.cert.org/archive/pdf/Botnets.pdf; *Barford/Yegneswaran*, "An Inside Look at Botnets", available at: http://pages.cs.wisc.edu/~pb/botnets_final.pdf; *Jones*, "BotNets: Detection and Mitigation".

641 See "Emerging Cybersecurity Issues Threaten Federal Information Systems", GAO, 2005, available at: http://www.gao.gov/new.items/d05231.pdf.

642 *Keizer*, Duch "Botnet Suspects Ran 1.5 Million Machines", TechWeb, 21.10.2005, available at http://www.techweb.com/wire/172303160

643 See *Weber*, "Criminals may overwhelm the web", BBC News, 25.01.2007, available at http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

644 E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, "Estonia under cyber attack", http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

645 "Over one million potential victims of botnet cyber crime", United States Department of Justice, 2007, available at: http://www.ic3.gov/media/initiatives/BotRoast.pdf.

646 *Staniford/Paxson/Weaver*, "How to Own the Internet in Your Space Time", 2002, available at: http://www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

647 *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International, 2006, page 142.

Электронные письма также показывают важность инструментов быстрого реагирования, которые можно тотчас же применить (см. Рисунок 33). Для слежения за подозреваемыми и их идентификации следователям часто требуется доступ к данным, которые могут быть удалены вскоре после их передачи[648]. Для успеха расследования зачастую очень важен короткий период реагирования органов охраны правопорядка. Без соответствующего законодательства и инструментов, позволяющих следователям действовать немедленно и предотвращать удаление данных, может быть невозможна эффективная борьба с киберпреступностью[649].

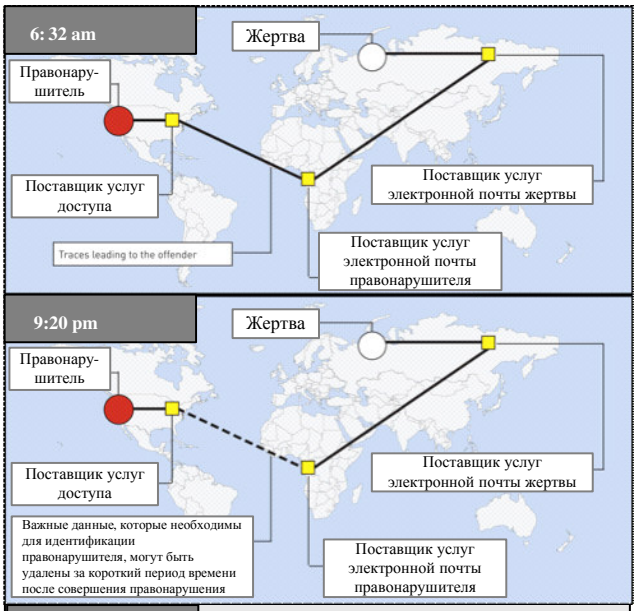


Рисунок 33

На графике показана важность немедленного реагирования в расследованиях киберпреступлений. Важные данные, создаваемые в процессе отправки электронных писем, и которые могут позволить идентифицировать злоумышленника, часто удаляются сразу после отправки электронного сообщения. Без доступа к этой информации идентификация злоумышленника зачастую невозможна.

"Процедуры быстрой заморозки"[650] и контактные центры сети[651] 24/7 – это примеры инструментов, которые могут ускорить расследования. Законы, направленные на сохранение данных, также направлены на увеличение времени, имеющегося в распоряжении органов охраны правопорядка для проведения расследований. Если данные, необходимые для слежения за злоумышленниками, сохраняются в течение определенного времени, органы охраны правопорядка имеют больше шансов успешно идентифицировать подозреваемых.

3.2.11 Скорость развития

Интернет постоянно меняется и развивается. Создание графического интерфейса пользователя (WWW[652]) стало началом существенного расширения, так как предыдущие услуги, вызываемые командами, были менее удобны для пользователей. Создание WWW позволило внедрить как новые приложения, так и новые преступления[653], органы охраны правопорядка стремятся не отставать. Дальнейшее развитие продолжается, особенно заметно оно в:

- онлайновых играх; и
- голосовой связи по IP-протоколу (VoIP).

Онлайновые игры всегда были более популярны, но неясно, могут ли органы охраны правопорядка успешно расследовать и наказывать преступления, совершаемые в этом виртуальном мире[654].

Переход от традиционной голосовой связи к интернет-телефонии также ставит новые проблемы для органов охраны правопорядка. Методы и процедуры, разработанные органами охраны правопорядка для перехвата обычных телефонных звонков, в целом неприменимы к VoIP. Перехват обычных голосовых звонков обычно осуществляется при помощи операторов связи. Применяя те же принципы к VoIP, органы охраны правопорядка должны действовать через поставщиков услуг интернета (ISP) и поставщиков услуг VoIP. Однако, если услуга основана на технологии прямой связи, поставщики услуг в целом не смогут

---

[648] *Gercke*, DUD 2003, 477 et seq.; *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

[649] Regarding the necessary instruments, see below: Chapter 6.2. One solution that is currently being discussed is data retention. Re the possibilities and risks of data retention, see: *Allitsch*, "Data Retention on the Internet – A measure with one foot offside?", Computer Law Review International 2002, page 161 et seq.

[650] The term "quick freeze" is used to describe the immediate preservation of data on request of law enforcement agencies. For more information, see below : Chapter 6.2.4.

[651] The 24/7 network point pursuant to Art. 35 Convention on Cybercrime is a contact point appointed to reply to requests from law enforcement agencies outside the country. For more information, see below: Chapter 6.3.8.

[652] The graphical user interface called World Wide Web (WWW) was created in 1989.

[653] The development of the graphical user interface supported content-related offences in particular. For more information, see above : Chapter 2.5.

[654] For more information see above: Chapter 2.5.5.

перехватывать сообщения, так как соответствующие данные передаются напрямую между участниками разговора[655]. Поэтому необходимы новые технологии[656].

Также быстро создаются новые аппаратные устройства с встроенными в них сетевыми технологиями. Новейшие домашние развлекательные системы превращают телевизоры в точки доступа в интернет, и последние модели мобильных телефонов могут хранить данные и соединяться с интернетом через беспроводные сети[657]. Устройства памяти USB (универсальной последовательной шины) с объемом памяти более 1 ГБ встраиваются в часы, ручки и карманные ножи. Органы охраны правопорядка в своей работе должны учитывать эти разработки, очень важно обучать офицеров, постоянно участвующих в расследованиях киберпреступлений, чтобы они были в курсе новейших технологий и могли определять соответствующие аппаратные средства и любые устройства, которые необходимо конфисковать.

Еще одной проблемой является использование точек беспроводного доступа. Расширение беспроводного доступа в интернет в развивающихся странах является как возможностью, так и проблемой для органов охраны правопорядка[658]. Если злоумышленники используют точки беспроводного доступа, которые не требуют регистрации, органам охраны правопорядка сложнее выследить злоумышленников, так как расследование выведет только к точке доступа.

3.2.12 Анонимная связь

Некоторые услуги интернета затрудняют выявление преступников[659]. Возможность анонимной связи является либо побочным продуктом услуги, либо предлагается с целью избежать неудобств для пользователя. Примерами подобных услуг, а также их сочетаний являются (см. Рисунки 34 и 35):

- терминалы выхода в интернет общего пользования, например терминалы в аэропорту или интернет-кафе[660];
- беспроводные сети[661];
- оплата услуг подвижной связи, которая не нуждается в регистрации;
- объем данных домашней страницы, доступный без регистрации;
- анонимные серверы связи[662];
- анонимные ретрансляторы[663].

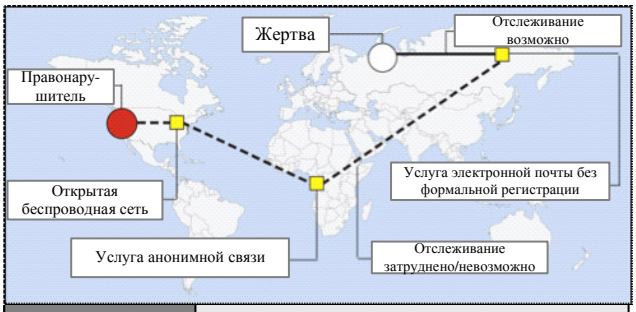


Рисунок 34

На рисунке показано, как преступники могут достичь анонимности путем сочетания различных подходов. Использование открытых беспроводных сетей делает практически невозможным выявление нарушителей. Использование услуги анонимной связи и услуги электронной почты, в которых не проверяются регистрационные данные, преступник может снизить шансы своего выявления.

655 Regarding the interception of VoIP by law enforcement agencies, see *Bellovin and others*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

656 With regard to the interception of peer-to-peer based VoIP communications, law enforcement agencies need to concentrate on carrying out the interception by involving the Access Provider.

657 Regarding the implication of the use of cell phones as storage media on computer forensics, see: *Al-Zarouni*, "Mobile Handset Forensic Evidence: a challenge for Law Enforcement", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Al-Zarouni%20-%20Mobile%20Handset%20Forensic%20Evidence%20-%20a%20challenge%20for%20Law%20Enforcement.pdf.

658 On the advantages of wireless networks for the development of an IT infrastructure in developing countries, see: "The Wireless Internet Opportunity for Developing Countries", 2003, available at: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

659 Regarding the challenges related to anonymous communication see: *Sobel*, The Process that "John Doe" is Due: Addressing the Legal Challenge to Internet Anonymity, Virginia Journal of Law and Technology, Symposium, Vol.5, 2000, available at: http://www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

660 Re legislative approaches requiring identification prior to the use of public terminals, see Art. 7 of the Italian Decree-Law No. 144. For more information see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 et seq. and below: Chapter 6.2.14

661 Regarding the difficulties that are caused if offenders use open wireless networks, see above: Chapter 3.2.3 .

662 Regarding technical approaches in tracing back users of Anonymous Communication Servers based on the TOR structure see: Forte, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf;

Преступники могут скрыть свою идентичность, к примеру, используя поддельные адреса электронной почты[664]. Многие провайдеры предлагают бесплатные адреса электронной почты. В тех случаях, когда требуется введение персональной информации, ее невозможно проверить, так что пользователи могут регистрировать адреса электронной почты, не раскрывая идентичности. Анонимные адреса электронной почты могут быть полезными, например, если пользователи хотят вступить в политическую дискуссию, не раскрывая свою идентичность. Анонимная связь может вызвать антисоциальное поведение, но она также может позволить пользователям действовать более свободно[665].

Принимая во внимание различные следы, оставляемые пользователями, становится ясной необходимость включения в основную деятельность инструментов, предотвращающих действия пользователей в своем профиле[666]. Поэтому различные государства и организации поддерживают принцип анонимного использования услуг электронной почты через интернет, например, этот принцип описан в Директиве Европейского союза о неприкосновенности частной жизни и электронных сообщений[667]. Один из примеров правового подхода к защите конфиденциальности пользователей можно найти в Статье 37 Регламента Европейского союза о защите данных[668]. Тем не менее, некоторые страны занимаются решением проблем анонимной связи путем введения правовых ограничений[669], одним из примеров является Италия, где поставщики услуг доступа к интернет общего пользования требуют идентификации пользователей до того, как они начнут пользоваться услугой[670].

Рисунок 35

На графике показано, как информация может быть скрыта на картинке. Шифрование программного обеспечения включает в себя информацию об изменении цвета некоторых пикселей. Если изображение достаточно большое, без доступа к оригинальному изображению с трудом можно понять было ли оно изменено. Использую эту технологию, правонарушители могут скрыть тот факт, что они обмениваются дополнительной информацией.

Эти меры направлены на содействие правоохранительным органам в деле выявления подозреваемых, но их можно легко обойти – преступники могут использовать незащищенные частные беспроводные сети или SIM-карты из стран, где не требуется регистрация. Неясно, будет ли ограничение анонимной связи и анонимного доступа к интернет играть более важную роль в стратегиях кибербезопасности[671].

---

663 See: *Claessens/Preneel/Vandewalle*, 'solutions for Anonymous Communication on the Internet", 1999.

664 Regarding the possibilities of tracing offenders using e-mail headers, see: *Al-Zarouni*, "Tracing Email Headers", 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Al-Zarouni.pdf.

665 *Donath*, 'sociable Media", 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

666 Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues". Regarding the benefits of anonymous communication see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

667 (33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services [...]. Source: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

668 Article 37 - Traffic and billing data 1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection. - Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

669 See below: Chapter 6.2.11.

670 Decree-Law 27 July 2005, no. 144. – Urgent measures for combating international terrorism. For further information on the Decree-Law, see, for example, the article "Privacy and data retention policies in selected countries", available at: http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

671 Regarding the technical discussion about traceability and anonymity, see: "CERT Research 2006 Annual Report", page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

3.2.13 Технология шифрования

Еще одним фактором, который может осложнить расследование киберпреступлений является технология шифрования[672], которая защищает информацию от несанкционированного доступа людей и является одним из основных технических решений в области борьбы с киберпреступностью[673]. Как и анонимность, шифрование не является чем-то новым[674], но компьютерные технологии изменили его смысл. Теперь существует возможность шифрования компьютерных данных одним щелчком мыши, что затрудняет взлом шифрования и данных доступа сотрудниками правоохранительных органов[675]. Неясно, в какой степени преступники уже используют технологию шифрования для маскировки своей деятельности, например, было сообщено о том, что террористы используют технологию шифрования[676]. В одном обзоре по детской порнографии сказано, что только 6% арестованных владельцев детской порнографии использовали технологию шифрования[677], однако эксперты подчеркивают угрозу все более широкого использования технологии шифрования в делах о киберпреступлениях[678].

Существуют средства для взлома шифров[679]. Различные программные продукты позволяют пользователям защитить файлы от несанкционированного доступа[680]. Если следователи имеют доступ к программному обеспечению, использованному для шифрования файлов, они смогут произвести дешифрование, но взломать шифр зачастую сложно и требует много времени[681]. В противном случае, шифр можно взломать, например, применив метод перебора всех возможных вариантов[682].

В зависимости от метода шифрования и размеров ключа для взлома шифра могут потребоваться десятилетия[683]. К примеру, если злоумышленник использовал программное обеспечение с 20-битовым шифром, то количество возможных значений ключа около миллиона. Использование компьютерной обработки с частотой один миллион операций в секунду позволит взломать шифр менее чем за секунду. Однако, если преступники используют 40-битный шифр, то для взлома шифра может потребоваться более двух недель[684]. При использовании 56-битного шифра для его взлома одному компьютеру потребуется более 2285 лет. Если преступники используют 128-битовый шифр, то для его взлома миллиарду компьютерных

---

672 Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/ Publications/Computer_Forensics_Past_Present_Future.pdf.

673 74 per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: "2006 E-Crime Watch Survey", page 1, available at: http://www.cert.org/archive/pdf/ecrimesurvey06.pdf

674 *Singh*; "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography", 2006; *D'Agapeyen*, "Codes and Ciphers – A History of Cryptography", 2006; "An Overview of the History of Cryptology", available at: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

675 Regarding the consequences for the law enforcement, Denning observed: "The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating". Excerpt from a presentation given by Denning, "The Future of Cryptography", to the joint Australian/OECD conference on Security, February, 1996. Regarding practical approaches to recover encrypted evidence see: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

676 Regarding the use of cryptography by terrorists, see: *Zanini/Edwards*, "The Networking of Terror in the Information Age", in *Arquilla/Ronfeldt*, "Networks and Netwars: The Future of Terror, Crime, and Militancy", page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf. *Flamm*, "Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography", available at: http://www.terrorismcentral.com/Library/Teasers/Flamm.html.

677 See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 9, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

678 *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: http://www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

679 Regarding the most popular tools, see: *Frichot*, "An Analysis and Comparison of Clustered Password Crackers", 2004, page 3, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Frichot-1.pdf; Regarding practical approaches in responding to the challenge of encryption see: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf ;

680 Examples include the software Pretty Good Privacy (see http://www.pgp.com) or True Crypt (see http://www.truecrypt.org).

681 See "Data Encryption, Parliament Office for Science and Technology No. 270", UK, 2006, page 3, available at: http://www.parliament.uk/documents/upload/postpn270.pdf.

682 Brute force attack is one method of defeating a cryptographic scheme by trying a large number of possible codes.

683 *Schneier*, "Applied Cryptography", Page 185; *Bellare/Rogaway*, "Introduction to Modern Cryptography", 2005, page 36, available at: http://www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

684 1099512 seconds.

систем, работающих только над проблемой дешифровки, потребуются тысячи миллиардов лет[685]. Последняя версия известного программного обеспечения для шифрования PGP обеспечивает 1024-битовое шифрование.

Современное программное обеспечение шифрования вышло далеко за пределы шифрования отдельных файлов. К примеру, последняя версия операционной системы Microsoft позволяет произвести шифрование всего жесткого диска[686]. Пользователи могут легко установить программы шифрования. Хотя некоторые компьютерные судебные эксперты считают, что эта функция их работе не угрожает[687], широкая доступность этой технологии для любого пользователя может привести к более широкому использованию шифрования. Доступны также средства для шифрования сообщений, например электронной почты, а телефонные вызовы[688] могут передаваться с использованием VoIP[689]. При использовании технологии шифрованной VoIP передачи, правонарушители могут защитить голосовые разговоры от перехвата[690].

Кроме того, разные методы могут быть объединены. Используя программные средства, преступники могут шифровать сообщения и передавать их в составе фотографии или картинки, эта технология называется стеганография[691]. Следственным органам трудно отличить безобидный обмен отпускными фотографиями от передачи фотографий с зашифрованными скрытыми сообщениями[692].

Доступность и применение преступниками технологий шифрования является проблемой для правоохранительных органов. В настоящее время обсуждаются различные правовые подходы к решению этой проблемы[693], в том числе возможные обязательства разработчиков программного обеспечения по установке лазейки для сотрудников правоохранительных органов, ограничение размеров ключа и обязанность разглашать ключи в случае уголовного расследования[694]. Однако технология шифрования используется не только преступниками: существуют различные способы использования такой технологии в законных целях. Защита конфиденциальной информации может быть затруднена без надлежащего доступа к технологии шифрования. Учитывая растущее число атак[695], защита является важным элементом кибербезопасности.

---

685 Equivalent to 10790283070806000000 years.

686 This technology is called BitLocker. For more information, see: "Windows Vista Security and Data Protection Improvements", 2005, available at: http://technet.microsoft.com/en-us/windowsvista/aa905073.aspx.

687 See *Leyden*, "Vista encryption 'no threat' to computer forensics", The Register, 02.02.2007, available at: http://www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

688 Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, "Skype Security Evaluation", 2005, available at: http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

689 Phil Zimmermann, the developer of the encryption software PGP developed a plug-in for VoIP software that can be used to install added encryption, in addition to the encryption provided by the operator of the communication services. The difficulty arising from the use of additional encryption methods is the fact that, even if the law enforcement agencies intercept the communications between two suspects, the additional encryption will hinder the analysis. For more information on the software, see: *Markoff*, "Voice Encryption may draw US Scrutiny", New York Times, 22.05.2006, available at: http://www.nytimes.com/2006/05/22/technology/22privacy.html?ex=1305950400&en=ee5ceb136748c9a1&ei=5088
Regarding the related challenges for law enforcement agencies, see: *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

690 *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

691 For further information, see: *Provos/Honeyman*, "Hide and Seek: An Introduction to Steganography", available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, "Image Steganography: Concepts and Practice", available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; Labs, "Developments in Steganography", available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, "On The Limits of Steganography", available at: http://www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; Curran/Bailey, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

692 For practical detection approaches see: *Jackson/Grunsch/Claypoole/Lamont*, Blind Steganography Detection Using a Computational Immune: A Work in Progress, International Journal of Digital Evidence, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV, 4675, page 1 et seq.; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001.

693 See below: Chapter 6.2.9.

694 See below: Chapter 6.2.9.

695 See above: Chapter 3.2.8.

3.2.14 Резюме

Расследование и судебное преследование киберпреступлений представляет ряд трудностей для правоохранительных органов. Это имеет жизненно важное значение не только для обучения людей, участвующих в борьбе с киберпреступностью, но и для разработки адекватного и эффективного законодательства. В этом разделе рассмотрены основные задачи повышения кибербезопасности и области, где существующих инструментов может оказаться недостаточно, а также введение специальных документов, которые могут оказаться необходимыми.

3.3 Правовые проблемы

3.3.1 Проблемы с подготовкой национальных уголовных законов

Надлежащее законодательство является основой расследования и уголовного преследования киберпреступности. Однако законодатели должны постоянно реагировать на развитие интернета и следить за эффективностью существующих положений, особенно с учетом быстрого развития сетевых технологий.

Исторически сложилось так, что внедрение услуг с использованием компьютера и технологий, связанных с интернетом породило новые формы преступности, вскоре после того как технология была внедрена. Одним из примеров является разработка в 1970-х годах компьютерных сетей, после чего вскоре произошел первый несанкционированный доступ к компьютерным сетям[696]. Точно также первые преступления, связанные с программным обеспечением, появились вскоре после появления в 1980-е годы персональных компьютеров, когда эти системы использовались для того, чтобы скопировать программные продукты.

Для того чтобы внести изменения в национальное уголовное законодательство, преследующие судебным порядком новые формы киберпреступлений, совершенных в режиме онлайн, требуется определенное время, некоторые страны еще не закончили этот процесс внесения изменений. Преступления, которые преследуются судебным порядком согласно национальному уголовному законодательству, должны быть рассмотрены и обновлены, например цифровая информация должна иметь статус, эквивалентный традиционным подписям и печатным документам[697]. Без внесения в законы преступлений, связанных с киберпреступностью, эти нарушения не могут быть преследованы по суду.

Главной проблемой для национальных уголовных правовых систем является длительное время между признанием потенциальных нарушений, совершаемых с использованием новых технологий, и внесением необходимых поправок в национальное уголовное законодательство. Эта проблема всегда остается важной и актуальной всегда, так как растет скорость инноваций в сети. Многие страны упорно работают над тем, чтобы законодательство шло в ногу с прогрессом[698]. В основном процесс регулирования состоит из трех этапов.

Внесение изменений в национальные законы должно начинаться с распознавания неправильного использования новой технологии. В органах охраны правопорядка нужно создать специальные отделы, которые умели бы расследовать потенциальные киберпреступления. Еще больше улучшит ситуацию развитие групп реагирования на компьютерные происшествия (CERT[699]), групп по расследованию компьютерных инцидентов (CIRT), групп реагирования на инциденты в сфере компьютерной безопасности (CSIRT) и других исследовательских учреждений.

Вторым шагом является выявление пробелов в Уголовном кодексе. Для того чтобы гарантировать наличие эффективного базового законодательства, необходимо сравнить статус уголовно-правовых положений с требованиями национального закона, являющимися результатом новых видов уголовных преступлений. Во многих случаях существующие законы могут охватывать новые варианты существующих преступлений, например законы, касающиеся подделки могут так же с легкостью распространяться и на электронные

---

696 See BBC News, “Hacking: A history”, 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

697 An example of the integration of digital sources is Section 11, Subsection 3 of the German Penal Code: “Audio & visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection.”

698 Within this process the case law based Anglo-American Law System shows advantage with regard to the reaction time.

699 Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 percent of internet systems to a halt in November 1988. For more information on the history of the CERT CC see: http://www.cert.org/meet_cert/; Goodman, Why the Police don’t Care about Computer Crime, Harvard Journal of Law and Technology, Vol. 10, Issue 3, page 475.

документы. Необходимость в законодательных поправках ограничена теми преступлениями, которые пропущены или недостаточно охвачены национальным законом.

Третьим шагом является разработка проекта нового законодательства. На основе имеющегося опыта, из-за быстрого развития сетевых технологий и их сложных структур, национальному правительству может быть затруднительно разработать проект законов по киберпреступности без международного сотрудничества[700]. Составление отдельного законодательства по киберпреступности может привести к существенному дублированию и бессмысленной трате ресурсов, а также необходимости следить за развитием международных стандартов и стратегий. Без международной гармонизации национальных уголовно-правовых положений борьба с транснациональной киберпреступностью будет встречать серьезные трудности из-за непоследовательных или несовместимых национальных законодательств. Следовательно, международные попытки гармонизировать различные национальные уголовные законы приобретают все большее значение[701]. Национальный закон может извлечь большую пользу из опыта других стран и юридической консультации международных экспертов.

3.3.2 Новые преступления

В большинстве случаев преступления, совершенные с использованием ИКТ, не являются новыми преступлениями, но мошенничества меняются так, чтобы их можно было совершить в онлайновом режиме. Один из примеров мошенничества таков: нет большой разницы между человеком, отправляющим письмо с намерением ввести в заблуждение другого человека, и аналогичным электронным письмом[702]. Если мошенничество уже является уголовным преступлением, то для судебного преследования таких деяний может не требоваться вносить изменения в национальный закон.

Ситуация меняется, если совершенные действия существующими законами не рассматриваются. В прошлом некоторые страны имели соответствующие положения для обычного мошенничества, но не имели возможности бороться с преступлениями, направленные против компьютерной системы, а не человека. Для этих стран потребовалось принять новые законы, устанавливающие судебное преследование мошенничества с использованием компьютера, в дополнение к обычному мошенничеству. Многочисленные примеры показывают, что расширенное толкование существующих положений не может заменить собой принятие новых законов.

Помимо регулирования, применимого к уже известным видам мошенничества, законодатели должны непрерывно анализировать новые и развивающиеся типы киберпреступлений, с тем чтобы обеспечить их эффективное судебное преследование. Одним из примеров киберпреступлений, к которым еще не во всех странах применяется судебное преследование, является воровство и мошенничество в компьютерных и онлайновых играх[703].
В течение долгого времени обсуждения относительно онлайновых игр сосредотачивались на проблемах защиты малолетних, например, требовали проверки возраста, и на незаконном контенте, например доступе к детской порнографии в онлайновой игре "Вторая жизнь"[704]. Постоянно обнаруживаются новые преступные действия: виртуальные деньги в онлайновых играх могут быть "украдены" и проданы на аукционе[705]. Некоторые виртуальные деньги имеют цену в реальных деньгах, в соответствии с обменным курсом, давая преступлению "реальное" измерение[706]. Такие преступления могут не во всех странах преследоваться по суду. Чтобы предотвратить существование зон безопасности для правонарушителей, жизненно важно наблюдать за развитием событий во всем мире.

3.3.3 Расширение использования ИКТ и необходимость в новых инструментах расследования

Правонарушители по-разному используют ИКТ для подготовки и совершения своих преступлений[707]. Органам охраны правопорядка необходимы соответствующие инструменты для расследования

---

700 Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and the UN Resolution 55/63.
701 See below: Chapter 5.
702 See above: Chapter 2.7.1.
703 Regarding the offences recognised in relation to online games see above: Chapter 2.5.5.
704 Regarding the trade of child pornography in Second Life, see for example BBC, "Second Life "child abuse" claim", 09.05.2007, at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6638331.stm; Reuters, Virtual Child Pornography illegal in Italy, 23.02.2007, at: http://secondlife.reuters.com/stories/2007/02/23/virtual-child-porn-illegal-in-italy/.
705 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 et seqq;
706 *Reuters*, "UK panel urges real-life treatment for virtual cash", 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.
707 Re the use of ICTs by terrorist groups, see: *Conway*, "Terrorist Use of the Internet and Fighting Back", Information and Security, 2006, page 16. *Hutchinson*, "Information terrorism: networked influence", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf. *Gercke*, "Cyberterrorism", Computer Law Review International 2007, page 64.

потенциальных уголовных действий. Некоторые инструменты, например хранение данных[708], могут нарушать права обычных пользователей интернета[709]. Если тяжесть уголовного преступления не пропорциональна интенсивности вмешательства, то использование инструментов расследования может быть необоснованным или незаконным. В результате, некоторые инструменты, которые могли бы улучшить расследование во многих странах не могут быть внедрены.

Внедрение инструментов расследования всегда является результатом компромисса между преимуществами для органов охраны правопорядка и вмешательством в права невинных пользователей интернета. Для того чтобы оценить изменение уровня угрозы важно следить за происходящими преступными действиями. Часто внедрение новых инструментов оправдывалось "борьбой против терроризма", но это по большей части больше побуждения, чем конкретное обоснование по существу.

3.3.4 Разработка процедур для цифровых доказательств

В частности, из-за низких цен[710] по сравнению с хранением физических документов, число цифровых документов увеличивается[711]. Оцифровка и растущее использование ИКТ оказывают большое влияние на процедуры, связанные со сбором доказательств и их использованием в суде[712]. В результате этого была введена разработка цифровых доказательств как новый источник доказательства[713]. Они определены как любые данные, сохраненные или переданные при помощи компьютерной технологии, которая поддерживает версию того, как совершено преступление[714]. Обработка цифровых доказательств сопровождается специфическими проблемами и требует определенных процедур[715]. Один из наиболее сложных аспектов заключается в поддержании целостности цифровых доказательств[716]. Цифровые данные весьма хрупкие и могут быть легко удалены[717] или изменены. Это особенно важно для информации, хранившейся в системной памяти RAM, которая автоматически удаляется при выключении системы[718] и поэтому требует специальных методов сохранения[719]. Кроме того, новые разработки могут оказать большое влияние на распределение цифровых доказательств. Примером является облачная обработка данных. В прошлом следователи, когда искали компьютерные данные, могли сосредоточиться на жилище подозреваемого. Сегодня они должны учитывать что цифровая информация могла храниться за границей, доступ к ней может быть только удаленным доступ и осуществляться в случае необходимости[720].

Цифровые доказательства играют важную роль в расследовании киберпреступлений. В целом можно отделить четыре фазы[721]:

- идентификация цифровых доказательств[722];

---

[708] Data retention describes the collection of certain data (such as traffic data) through obliged institutions e.g., Access Providers. For more details, see below: Chapter 6.2.5.

[709] Related to these concerns, see: “Advocate General Opinion”, 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top.

[710] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol.X, No.5.

[711] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[712] *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

[713] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; Regarding the historic development of computer forensics and digital evidence see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist’s View, International Journal of Digital Evidence, 2002, Vol.1, No.1.

[714] *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: http://www.cybex.es/agis2005/elegir_idioma_pdf.htm.

[715] Regarding the difficulties of dealing with digital evidence on the basis of the traditional procedures and doctrines see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 et seq.

[716] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

[717] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[718] *Nolan/O’Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[719] See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

[720] *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

[721] Regarding the different models of Cybercrime investigations see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol.3, No.1; See as well *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1 who are differentiating between six different phases.

- сбор и сохранение доказательств[723];
- анализ компьютерной технологии и цифровые доказательства; и,
- представление доказательства в суде.

Кроме процедур, которые касаются представления цифрового доказательства в суде, особого внимания требуют пути, которыми эти цифровые доказательства собраны. Сбор цифровых доказательств связан с компьютерно-судебной экспертизой. Термин "компьютерно-судебная экспертиза" описывает систематический анализ оборудования ИТ с целью поиска цифровых доказательств[724]. Относительно того факта, что количество данных, сохраненных в цифровом формате, постоянно увеличивается, на первый план выходят логистические проблемы таких расследований[725]. Поэтому подходы к автоматизированным судебным процедурам, например, поиск известных детских порнографических изображений[726] или поиск ключевого слова[727], основанный на значения хэш-функции, играют важную роль в дополнение к ручным расследованиям[728].

В зависимости от требования конкретного расследования, компьютерно-судебная экспертиза может, например, включать в себя следующее:

- анализ аппаратных и программных средств, используемых подозреваемым[729];
- помощь следователям в идентификации соответствующего доказательства[730];
- восстановление удаленных файлов[731];
- расшифровка файлов[732]; и,
- идентификация пользователей интернета при помощи анализа данных о трафике[733].

---

722 This includes the development of investigation strategies

723 The second phase does especially cover the work of the so-called „First responder“ and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

724 See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol.1, No.2, page 3.

725 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol 119, page 532.

726 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

727 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

728 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

729 This does for example include the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

730 This does for example include the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

731 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

732 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encrpytion Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3. Regarding the decryption process within forensic investigations see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

733 Regarding the differnet sources that can be used to extract traffic data see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 et seq.

4 СТРАТЕГИИ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ

Растущее число раскрытых киберпреступлений и технических инструментов для автоматического совершения киберпреступлений, включая системы анонимного обмена файлами[734] и программные продукты, предназначенные для создания компьютерных вирусов[735], означает, что борьба с киберпреступностью стала важнейшим элементом деятельности органов охраны правопорядка по всему миру. Киберпреступность представляет собой проблему для органов охраны правопорядка и в развитых, и в развивающихся странах. Поскольку ИКТ стремительно развиваются, особенно в развивающихся странах, становится важным создание и внедрение стратегии эффективной борьбы с киберпреступностью в рамках национальной стратегии кибербезопасности.

4.1 Законодательство о киберпреступности как часть стратегии борьбы с киберпреступностью

Как отмечалось ранее, кибербезопасность[736] играет важную роль в непрерывном развитии информационных технологий, в той же мере, что и услуги интернета[737]. Создание безопасного интернета и защиты пользователей интернета стало составной частью разработки и новых услуг, и государственной политики[738]. Стратегии кибербезопасности, например, разработка систем технической защиты или обучение пользователей, для того чтобы они не стали жертвами киберпреступности, может помочь снизить риск киберпреступности[739].

Стратегия борьбы с киберпреступностью должна стать неотъемлемым элементом стратегии кибербезопасности. Глобальная программа кибербезопасности МСЭ[740], как глобальная основа для диалога и международного сотрудничества, координирует международное реагирование на растущие проблемы в области кибербезопасности и повышает уверенность и безопасность в информационном обществе, формирует текущую работу, инициативы и партнерства с целью создания глобальных стратегий для решения этих связанных задач. Все необходимые меры распределены по пяти принципам Глобальной программы кибербезопасности, которые важны в любой стратегии кибербезопасности. Кроме того, способность к эффективной борьбе с киберпреступностью требует принятия мер, которые будут приниматься в рамках всех пяти принципов[741].

---

[734] *Clarke/Sandberg/Wiley/Hong*, "Freenet: a distributed anonymous information storage and retrieval system", 2001; *Chothia/Chatzikokolakis*, "A Survey of Anonymous Peer-to-Peer File-Sharing", available at: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Design", 2005. See also above: Chapter 3.2.l.

[735] For an overview about the tools used, see *Ealy*, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", available at: http://www.212cafe.com/download/e-book/A.pdf. For more information, see above: Chapter 3.2.h.

[736] The term "Cybersecurity" is used to summarise various activities such as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. Regarding the definition of cybersecurity, ITU-T Recommendation X.1205 "Overview of Cybersecurity" provides a definition, description of technologies, and network protection principles. "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: Availability; Integrity, which may include authenticity and non-repudiation; Confidentiality." Also see *ITU*, List of Security-Related Terms and Definitions, available at: http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00000A0002MSWE.doc.

[737] With regard to development related to developing countries see: ITU Cybersecurity Work Programme to Assist Developing Countries 2007-2009, 2007, available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-cybersecurity-work-programme-developing-countries.pdf.

[738] See for example: ITU WTSA Resolution 50: Cybersecurity (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52: Countering and combating spam (Rev. Johannesburg, 2008) available at: http://www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45: Mechanism for enhancing cooperation on cybersecurity, including combating spam (Doha, 2006) available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; EU Communication towards a general policy on the fight against cyber crime, 2007 available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization, President's Information Technology Advisory Committee, 2005, available at: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[739] For more information see *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

[740] For more information see: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[741] See below: Chapter 4.4.

4.2 Реализация существующих стратегий

Одна из перспективных стратегий борьбы с киберпреступностью, разработанная в промышленно-развитых странах, может быть внедрена в развивающихся странах, что позволит сократить расходы и время на развитие собственных стратегий. Реализация существующих стратегий может позволить развивающимся странам использовать существующие знания и опыт.

Тем не менее, реализация существующих стратегий борьбы с киберпреступностью создает ряд трудностей. Несмотря на то, что и развивающиеся, и развитые страны сталкиваются с похожими проблемами, оптимальные решения, которые могут быть приняты, зависят от ресурсов и возможностей каждой страны. Промышленно развитые страны могут повысить уровень кибербезопасности более гибкими способами, например, сосредотачиваясь на внедрении более дорогостоящей технической защиты.

Существует несколько других вопросов, которые должны быть приняты во внимание в развивающихся странах, применяющих у себя существующие стратегии борьбы с киберпреступностью:

- совместимость соответствующих законодательных систем;
- статус инициатив поддержки, например обучение общества;
- степень мер самозащиты на месте; и
- степень поддержки частного сектора, среди прочих вопросов, например через частно-государственное партнерство.

4.3 Региональные различия

Учитывая международный характер киберпреступности, в борьбе с киберпреступностью жизненно важное значение имеет гармонизация национальных законодательств и техники. Однако гармонизация должна учитывать региональные требования и возможности. Большое значение региональных аспектов в осуществлении стратегий борьбы с киберпреступностью подчеркивает тот факт, что многие правовые и технические стандарты были согласованы между промышленно развитыми странами и не включали некоторые важные аспекты для развивающихся стран[742]. Таким образом, для их реализации в других странах в них должны быть включены региональные факторы и различия.

4.4 Соответствие проблем киберпреступности основам кибербезопасности

Глобальная программа кибербезопасности преследует семь основных целей, основанных на пяти принципах: 1) Правовые меры; 2) Технические и процедурные меры; 3) Организационные структуры; 4) Создание потенциала; и 5) Международное сотрудничество. Как отмечалось выше, вопросы, связанные с киберпреступностью, играют важную роль во всех пяти принципах Глобальной программы кибербезопасности. Среди этих областей деятельности, работа в области правовых мер сосредоточена на том, как решать нахождение законодательные проблемы, поставленные преступными деяниями, совершаемыми в сетях ИКТ в международном масштабе.

4.4.1 Правовые меры

Среди пяти принципов, при рассмотрении стратегии борьбы с киберпреступностью, вероятно, правовые меры являются наиболее важными. Во-первых, эти меры требуют принятия основных положений уголовного законодательства, предусматривающих уголовную ответственность за такие действия, как компьютерное мошенничество, незаконный доступ, искажение данных, нарушение авторских прав и детская порнография[743]. Тот факт, что существуют положения, предусмотренные Уголовным кодексом за аналогичные деяния, совершенные не в сети, не означает, что они могут применяться к деяниям,

[742] The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States of America, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arabic regions.

[743] *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview about the most important substantive criminal law provisions see below: Chapter 6.1.

совершенным в интернете[744]. Таким образом, для выявления любых возможных пробелов жизненно важное значение имеет тщательный анализ существующих национальных законов[745]. Помимо основных положений Уголовного законодательства[746], правоохранительные органы нуждаются в необходимых механизмах и инструментах для расследования киберпреступлений[747]. Подобные расследования сами по себе представляют сложные задачи[748]. Преступники могут действовать практически из любого места в мире и принимать меры, чтобы скрыть свою личность[749]. Механизмы и инструменты, необходимые для расследования киберпреступлений могут существенно отличаться от используемых для расследования общих уголовных преступлений[750]. В связи с международным масштабом[751] киберпреступности необходимо дополнительно разработать основу национального законодательства, с тем чтобы иметь возможность совместного сотрудничества с правоохранительными органами за рубежом[752].

4.4.2 Технические и процедурные меры

Расследование киберпреступлений показало, что очень часто они имеют значительную техническую составляющую[753]. В дополнение к требованию защиты целостности доказательств в ходе расследования требуются точно определенные процедуры. Разработка необходимого потенциала и процедур является необходимым требованием, касающимся борьбы с киберпреступностью.

Еще одна проблема заключается в разработке технических средств защиты. Хорошо защищенные компьютерные системы труднее атаковать. Важным первым шагом является совершенствование технической защиты путем внедрения надлежащих стандартов. Например, изменения в системе виртуального банка, например переход от TAN[754] к ITAN[755], позволит устранить большую часть опасностей, исходящих от сегодняшних фишинг-атак, это демонстрирует жизненно важное значение технических решений[756].

---

744 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 et. Seqq.

745 For an overview of the cybercrime-related legislation and their compliance with the international standards defined by the Convention on Cybercrime see the country profiles provided on the Council of Europe website. Available at: http://www.coe.int/cybercrime/. [745] See for example the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005 -, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf ;*Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.* , available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework - unauthorized access to computer systems - penal legislation in 44 countries, available at: http://www.mosstingrett.no/info/legal.html.

746 See below: Chapter 6.1.

747 See below: Chapter 6.1.

748 For an overview about the most relevant challenges in the fight against Cybercrime see below: Chapter 3.1.

749 One possibility to mask the identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, 'solutions for Anonymous Communication on the Internet", 1999; Regarding the technical discussion about traceability and anonymity, see: "CERT Research 2006 Annual Report", page 7 et seqq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf; Regarding anonymous file-sharing systems see: *Clarke/Sandberg/Wiley/Hong*, "Freenet: a distributed anonymous information storage and retrieval system", 2001; *Chothia/Chatzikokolakis*, "A Survey of Anonymous Peer-to-Peer File-Sharing", available at: http://www.spinellis.gr/pubs/jml/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao;Xiao*, "A Mutual Anonymous Peer-to-Peer Protocol Desing", 2005.

750 Regarding legal responses to the challenges of anonymous communication see below: Chapter 6.2.10 and Chapter 6.2.11.

751 See above: Chapter: 3.2.6.

752 See in this context below: Chapter 6.3.

753 *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf; Regarding the need for standardisation see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2;

754 Transaction Authentication Number – for more information, see: "Authentication in an Internet Banking Environment", United States Federal Financial Institutions Examination Council, available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

755 The ITAN system improves the TAN system. The financial institutions provide the customer with a number of TAN-indexed identity numbers. With regard to each relavant transaction, the online banking system requires a specific ITAN number selected at random from the list of supplied TAN. For more information, see: *Bishop*, "Phishing & Pharming: An investigation into online identity theft", 2005, available at: http://richardbishop.net/Final_Handin.pdf.

756 Re the various approaches of authentication in Internet banking, see: "Authentication in an Internet Banking Environment", United States Federal Financial Institutions Examination Council, available at: http://www.ffiec.gov/pdf/authentication_guidance.pdf.

Технические меры защиты должны включать защиту всех элементов технической инфраструктуры – инфраструктуру основной сети, а также множество персональных компьютеров, связанных по всему миру. Для защиты пользователей интернет и предприятий можно определить две потенциальных целевых группы:

- конечные пользователи и предприятия (прямой подход); и
- поставщики услуг и компании, разрабатывающие программное обеспечение.

В материально-техническом отношении может быть легче сосредоточить внимание на защите основной инфраструктуры, например, магистральной сети, маршрутизаторов, базовых услуг, а не на объединении миллионов пользователей в единую стратегию борьбы с киберпреступностью. Защита пользователя может осуществляться косвенно, путем защиты используемых потребительских услуг, например виртуального банка. Данный косвенный подход к защите пользователей интернета может сократить число людей и предприятий, которые должны быть включены в перечень этапов по обеспечению технической защиты.

Хотя желательно ограничить количество людей, у которых должна действовать техническая защита, пользователи компьютеров и интернета зачастую являются слабым звеном и главной мишенью преступников. Атаки на частные компьютеры для получения конфиденциальной информации, случаются чаще, чем на хорошо защищенные компьютерные системы финансовых учреждений. Несмотря на проблемы в материально-техническом отношении, защита инфраструктуры конечных пользователей является жизненно важным звеном в технической защите всей сети.

Поставщики услуг интернета и поставщики продукции, компании, разрабатывающие программное обеспечение, играют важную роль в поддержке стратегий борьбы с киберпреступностью. Из-за их прямого контакта с клиентами они могут действовать в качестве гаранта безопасности предприятия, например, распространяя средства защиты и информацию о текущем положении последних преступлений[757].

4.4.3 Организационные структуры

Эффективная борьба с киберпреступностью требует развитой организационной структуры. Не имея правильно созданных, которые позволяют избежать дублирования и основаны на четко определенных полномочиях, вряд ли можно проводить комплексные исследования, требующих содействия различных юридических и технических экспертов.

4.4.4 Создание потенциала и обучение пользователей

Киберпреступность представляет собой глобальное явление. Для того чтобы иметь возможность эффективно расследовать преступления, необходимо гармонизировать законодательства и разработать средства международного сотрудничества. В целях обеспечения действия мировых стандартов и в развитых, и в развивающихся странах необходимо создание потенциала[758].

В дополнение к созданию потенциала требуется обучить пользователей[759]. Некоторые киберпреступления, особенно те, которые связаны с мошенничеством типа "фишинг" и "спуфинг", как правило, обусловлены не отсутствием средств технической защиты, а неосведомленностью[760]. Существуют различные программные

---

[757] Regarding the approaches to coordinate the cooperation of law enforcement agencies and Internet Service Providers in the fight against Cybercrime see the results of the working group established by Council of Europe in 2007. For more information see: http://www.coe.int/cybercrime/.

[758] Capcity Buidling is in general defined as the creation of an enabling environment with appropriate policy and legal frameworks, institutional development, including community participation (of women in particular), human resources development and strengthening of managerial systems, adding that, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations and water user groups, professional associations, academics and others.

[759] At the G8 Conference in Paris in 2000, *Jean-Pieree Chevenement*, the French Minister of Interior, stated: “More broadly, we have to educate users. They must all understand what they can and can’t do on the Internet and be warned of the potential dangers. As use of the Internet grows, we’ll naturally have to step up our efforts in this respect.” Regarding user education approaches in the fight against Phishing, see: “Anti-Phishing Best Practices for ISPs and Mailbox Providers”, 2006, page 6, available at: http://www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, “Technical Trends in Phishing Attacks”, available at: http://www.cert.org/archive/pdf/Phishing_trends.pdf. Re sceptical views regarding user education, see: *Görling*, “The Myth Of User Education”, 2006, available at: http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[760] “Anti-Phishing Best Practices for ISPs and Mailbox Providers”, 2006, page 6, available at: http://www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, “Technical Trends in Phishing Attacks”, available at: http://www.cert.org/archive/pdf/Phishing_trends.pdf.

продукты, позволяющие автоматически определять некоторые мошеннические веб-сайты[761], однако до сих пор, эти продукты не могут выявить все подозрительные веб-сайты. Стратегия защиты пользователя, основанная только на программных продуктах, имеет ограниченные возможности защиты пользователей[762]. Несмотря на то, что средства технической защиты будут продолжать развиваться и доступные программные продукты будут регулярно обновляться, такие продукты пока еще не могут заменить другие подходы.

Одним из наиболее важных элементов в предупреждении киберпреступлений является обучение пользователя[763]. Например, если пользователи знают, что их финансовые учреждения никогда не будут связываться с ними по электронной почте с просьбой сообщить пароль или детали банковского счета, они не станут жертвами фишинга или атаки с целью кражи идентичности. Обучение пользователей интернета сокращает количество потенциальных целей нападения. Пользователи могут обучаться при помощи:

- общественных кампаний;
- на уроках в школе, в библиотеках, в информационных центрах и университетах;
- частно-государственного партнерства (PPP).

Одним из важных требований к эффективному обучению и информационной стратегии является открытое сообщение о новейших угрозах со стороны киберпреступности. Некоторые государственные и/или частные предприятия, для того чтобы избежать утраты доверия к сетевым онлайновым услугам, отказываются признавать, что их граждане и клиенты соответственно страдают от угроз киберпреступности. Федеральное бюро расследований Соединенных Штатов в прямой форме попросило компании преодолеть их неприязнь к негативному освещению и докладам о киберпреступности[764]. В целях определения уровня угрозы, а также для информирования пользователей, жизненно важно значение совершенствовать сбор и публикацию соответствующей информации[765].

4.4.5 Международное сотрудничество

Во многих случаях процессы передачи данных по интернету затрагивают несколько стран[766]. Это результат развития сети, а также того факта, что можно создать протоколы, обеспечивающие успешные передачи, даже если прямая линия связи временно заблокирована[767]. Кроме того, множество услуг интернета, например услуги хостинга, предлагаемых компаниям, базируются за рубежом[768].

---

761 *Shaw*, “Details of anti-phishing detection technology revealed in Microsoft Patent application”, 2007, available at: http://blogs.zdnet.com/ip-telephony/?p=2199. “Microsoft Enhances Phishing Protection for Windows”, MSN and Microsoft Windows Live Customers - Cyota Inc., Internet Identity and MarkMonitor to provide phishing Web site data for Microsoft Phishing Filter and SmartScreen Technology services, 2005, available at: http://www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

762 For a different opinion, see: *Görling*, “The Myth Of User Education”, 2006, at:http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

763 At the G8 Conference in Paris in 2000, *Jean-Pieree Chevenement*, the French Minister of Interior, stated: “More broadly, we have to educate users. They must all understand what they can and can’t do on the Internet and be warned of the potential dangers. As use of the Internet grows, we’ll naturally have to step up our efforts in this respect.”

764 “The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office.” See Heise News, 27.10.2007, available at: http://www.heise-security.co.uk/news/80152.

765 Examples of the publication of cybercrime-related data include: “Symantec Government Internet Security Threat Report Trends for July–December 06”, 2007, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf; Phishing Activity Trends, Report for the Month of April 2007, available at: http://www.antiphishing.org/reports/apwg_report_april_2007.pdf.

766 Regarding the extend of transnational attacks in the the most damaging cyber attacks see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

767 The first defined and still most important communication protocols are: TCP (Transmission Control Protocol) and the IP (Internet Protocol). For further information see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

768 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; Regarding the possibilities of network storage services see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

В тех случаях, когда жертвами преступника становятся люди из нескольких стран, для расследования требуется сотрудничество правоохранительных органов всех стран, где была совершена атака[769]. Международные и транснациональные расследования без согласия компетентных органов в соответствующих странах становятся затруднительными из-за принципа государственного суверенитета. Данный принцип в целом не позволяет стране проводить расследования на территории другой страны без разрешения местных властей[770]. Таким образом, расследования должны проводиться при поддержке властей всех затронутых стран. В связи с тем, что фактически в большинстве случаев успешное раскрытие преступления на месте возможно только в течение маленького интервала времени, то когда дело касается расследований киберпреступлений, применение классической правовой взаимопомощи становится затруднительным. Это объясняется тем фактом, что оказание взаимной правовой помощи в целом требует много времени для выполнения формальных процедур. Поэтому улучшения в плане расширения международного сотрудничества играют важную и решающую роль в развитии и реализации стратегий кибербезопасности и стратегий борьбы с киберпреступностью.

[769] Regarding the need for international cooperation in the fight against Cybercrime see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 et seqq. , available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seqq. , available at: http://media.hoover.org/documents/0817999825_1.pdf

[770] National Sovereignty is a fundamental principle in International Law. See Roth, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

5 ОБЗОР МЕЖДУНАРОДНЫХ ЗАКОНОДАТЕЛЬНЫХ ПОДХОДОВ

Следующая глава содержит обзор международных законодательных подходов[771] и их связи с региональными подходами.

5.1 Международные подходы

Во многих международных организациях ведется постоянная работа по анализу последних достижений киберпреступности, и созданы рабочие группы для разработки стратегии по борьбе с этими преступлениями.

5.1.1 Группа восьми[772]

В 1997 году Группа восьми (G8) создала Подкомитет[773] по высокотехнологичным преступлениям, рассматривающий проблемы борьбы с киберпреступностью[774]. Во время встречи Группы восьми в Вашингтоне, округ Колумбия, США, министры юстиции и внутренних дел Группы восьми приняли десять принципов и состоящий из десяти пунктов план действий по борьбе с высокотехнологичными преступлениями[775]. Позднее главы Группы восьми поддержали эти принципы, к которым относятся:

- для тех, кто злоупотребляет информационными технологиями не должно быть безопасных мест;
- расследование и судебное преследование международных высокотехнологичных преступлений должны быть согласованы между всеми заинтересованными государствами, независимо от того, где нанесен ущерб;
- сотрудники правоохранительных органов должны быть обучены и иметь оборудование для раскрытия высокотехнологичных преступлений.

В 1999 г. на Конференции министров по борьбе с транснациональной организованной преступностью в Москве, Российская Федерация, Группа восьми определила планы по борьбе с высокотехнологичными преступлениями[776]. Они выразили свою озабоченность по поводу таких преступлений, как детская порнография, а также по поводу отслеживания сделок и трансграничного доступа к хранимым данным. Их Коммюнике содержит ряд принципов по борьбе с киберпреступностью, которые сегодня содержатся в ряде международных стратегий[777].

---

771 This includes regional approaches.

772 The Group of Eight (G8) consists of eight countries: Canada, France, Germany, Italy, Japan, Great Britain, United States and the Russian Federation. The Presidency of the group that represents more than 60% of the world economy (Source: http://undp.org) rotates every year.

773 The idea of the creation of five Subgroups – among them, one on High-Tech Crimes – was to improve the implementation of the Forty Recommendations adopted by G8 Heads of State in 1996.

774 The establishment of the Subgroup (also described as the Subgroup to the "Lyon Group") continued the efforts of the G8 (at that time still G7) in the fight against organised crime, that started with the launch of the Senior Experts Group on Organised Crimes (the "Lyon Group") in 1995. At the Halifax summit in 199,5 the G8 expressed: "We recognize that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from drug trafficking and other serious crimes. To implement our commitments in the fight against transnational organized crime, we have established a group of senior experts with a temporary mandate to look at existing arrangements for cooperation both bilateral and multilateral, to identify significant gaps and options for improved coordination and to propose practical action to fill such gaps". See: Chairman's Statement, Halifax G7 Summit, June 17, 1995. For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

775 Regarding the G8 activities in the fight against Cybercrime see as well: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

776 "Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime", Moscow, 19-20 October, 1999.

777 14. As the use of the Internet and other new technologies increase, more criminals are provided with opportunities to commit crimes remotely, via telephone lines and data networks. Presently, malicious programming code and harmful communications (such as child pornography) may pass through several carriers located in different countries. And infrastructures such as banking and finance increasingly are becoming networked and thereby vulnerable to cyber-attack from distant locations. We convene today to provide additional personal attention to and direction for our joint action against this transnational criminality.
15. Our goals are to ensure that our people are protected from those who use new technologies for criminal purposes, such as child exploitation, financial crime, and attacks on critical infrastructures, and to ensure that no criminal receives safe haven anywhere in the world. We are determined that our law enforcement authorities have the technical ability and legal processes to find criminals who abuse technologies and bring them to justice. The safety of our people and their economic prosperity depend upon our leadership and determination and our ability to take coordinated action. We direct our experts to continue their work, particularly, on

Одним из практических достижений в работе экспертной группы стала разработка международных круглосуточных связей стран-участниц, требующих создания контактных центров для транснациональных расследований, которые доступны 24 часа в сутки 7 дней в неделю[778].

На конференции в Париже, Франция, в 2000 году Группа восьми обратилась к вопросу киберпреступности с призывом не допускать незаконных цифровых укрытий. Уже в то время эти попытки Группы восьми объединялись с международными решениями Конвенции Совета Европы о киберпреступности[779].

---

problems which arise for our law enforcement authorities from new developments in information technology and their use by criminals.
16. Strength of G-8 Legal Systems. Our experts have completed a comprehensive review of G-8 legal systems to assess whether those systems appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes. While, over the past decade, our governments have acted to see that their legal systems account for new technologies, there remains room for improvement. Where laws or legal processes require enhancements, we are committed to use best efforts to fill these gaps and, consistent with fundamental national legal principles, to promote new legal mechanisms for law enforcement to facilitate investigations and prosecutions.
17. Principles on Transborder Access to Stored Computer Data. Criminals take advantage of the jurisdictional inability of law enforcement authorities to operate across national borders as easily as criminals can. High-tech crimes may rapidly affect people in many countries, and evidence of these crimes, which may be quickly altered or destroyed, may be located anywhere in the world. Recognizing these facts, and taking into account principles relating to sovereignty and to the protection of human rights, democratic freedoms and privacy, our law enforcement authorities conducting criminal investigations should in some circumstances be able to pursue investigations across territorial borders. We have today adopted certain principles for access to data stored in a foreign state, which are contained in the Annex 1 to this Communique. We are committed to work towards implementation of these principles through international cooperation, including legal instruments, and through national laws and policies, and invite all nations to join in this effort. We note, however, that continued work is required in this area, including on the appropriate collection, preservation and disclosure of traffic data, and we direct our experts to make further progress in consultation with industry.
18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries. Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.
19. International Network of 24-hour Contacts. Our 24-hour points of contact network, which allows us to respond to fast-breaking investigations, has now been expanded from the eight G-8 countries to a number of additional countries around the world. The speed of electronic communications and perishability of electronic evidence requires real-time assistance, and this growing global network has dramatically increased our investigative abilities. We direct our experts to facilitate further growth of this network. G-8 nations and their partners should also use this network proactively to notify other countries when they learn of significant potential threats to our shared networks.
20. Criminality Associated with the 'Millennium Bug'. Our countries have been at the forefront of efforts to successfully tackle the 'Millennium Bug' or 'Y2K Problem', which presents a major threat to the increasingly networked global economy. We are concerned that the Millennium Bug may either provide new opportunities for fraud and financial crimes, or mask ongoing criminality, if systems for accounting and reporting are disrupted. Therefore, as part of our new proactive use of our 24-hour network, we will provide early warning of Y2K-related abuses.
21.Internet Fraud. We recognize that Internet fraud, in all of its forms, poses a significant threat to the growth and development of electronic commerce and to the confidence that consumers place in electronic commercial transactions. To counter this threat, we are undertaking a comprehensive response, including crime prevention, investigation, and prosecution. For example, we are sharing information on international Internet fraud schemes - including information relating to the criminals, their methods and techniques, the victims involved in these schemes, and reports of enforcement actions - so that criminals defrauding people in multiple countries are investigated and prosecuted for the full range of their criminal activities.

[778] The idea of a 24/7 Network has been picked up by a number of international approaches in the fight against cybercrime. One example is Article 35 of the Convention on Cybercrime:
(1) Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
a) the provision of technical advice;
b) the preservation of data pursuant to Articles 29 and 30;
c) the collection of evidence, the provision of legal information, and locating of suspects. […]

[779] *Jean-Pieree Chevenement*, the French Minister of Interior, stated: "Now that the G8 has provided the impetus, it's vital that we formalize the new legal rules and procedures for cooperation in a legal instrument applying world-wide. For France, the negotiations under way in the Council of Europe on a Convention on Cyber-Crime are of fundamental importance for several reasons. The draft currently under discussion defines the offences which all States would have to recognize. It goes on to propose ways in which they could cooperate, taking up, for example, the idea of national contact points. It also proposes extradition procedures. In short, this agreement is an essential instrument, which France wants to see concluded within a reasonable period of time. The important thing about these negotiations is that the countries involved include some major countries outside the Council of Europe and that, once signed, this convention will be opened for signature by all States wishing to accede to it. The idea is in fact to get a convention which applies world-wide so that there can be no more "digital havens" or "Internet havens" in which anyone wanting to engage in shady activities can find all the facilities they need, including financial ones, for laundering the product of their crimes. Since we must

В 2001 году Группа восьми обсудила инструменты и процедуры борьбы с киберпреступностью в ходе рабочего совещания, состоявшегося в Токио[780], обращая особое внимание на то, должны ли данные быть обязательно сохранены или сохранение данных является дополнительной мерой[781].

В 2004 году министры юстиции и внутренних дел Группы восьми опубликовали коммюнике, в котором выступили за необходимость создания глобального потенциала для борьбы с преступным использованием интернета[782]. Опять же Группа восьми сослалась на Конвенцию Совета Европы о киберпреступности[783].

На московском совещании министров юстиции и внутренних дел Группы восьми в 2006 году обсуждались вопросы, связанные с борьбой с киберпреступностью, проблемы киберпространства и особенно необходимость совершенствования эффективных контрмер[784]. За совещанием министров юстиции и внутренних дел Группы восьми последовал саммит Группы восьми в Москве, где обсуждалась[785] тема кибертерроризма[786].

В 2007 году на совещании Министров юстиции и внутренних дел Группы восьми в Мюнхене, Германия, также обсуждалась проблема использования интернета террористами, и участники согласились с необходимостью уголовного преследования террористических групп за неправомерное использование интернета[787]. Данное соглашение не включает в себя конкретные действия, которые считаются противозаконными в отдельных странах.

5.1.2 Организация объединенных наций[788]

На 8-м Конгрессе по предотвращению преступности и обращению с преступниками, состоявшемся в Гаване, Куба, с 27 августа по 7 сентября 1990 года, Генеральная Ассамблея ООН приняла резолюцию, касающуюся законодательства в области преступлений с использованием компьютера[789]. Основываясь на резолюции 45/121 (1990), в 1994 году ООН опубликовала руководство по профилактике и борьбе с преступлениями с использованием компьютера[790].

---

never lose sight of the fact that the Internet is a global system and that no country can isolate itself from the rules under which it has to operate."

780 G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

781 The experts expressed their concerns regarding implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible"; "Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers", G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001.

782 G8 Justice and Home Affairs Communiqué, Washington DC, May 11, 2004.

783 G8 Justice and Home Affairs Communiqué Washington DC, May 11, 2004:10. "Continuing to Strengthen Domestic Laws": To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations. With the Council of Europe Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis."

784 The participants expressed their intention to strengthen the instruments in the fight against Cybercrime: "We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors". See: http://www.g7.utoronto.ca/justice/justice2006.htm.

785 Regarding the topic Cyberterrorism see above: Chapter 2.8.1; In addition see See: *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; Lewis, "Cyber-terrorism and Cybersecurity"; http://www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, "Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy", in Arquilla/Ronfeldt, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 et seqq., available at: http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, "Cyberterrorism, Are We Under Siege?", American Behavioral Scientist, Vol. 45 page 1033 et seqq; United States Department of State, "Pattern of Global Terrorism, 2000", in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism", available at: http://www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, "Information Technology for Counterterrorism: Immediate Actions and Future Possibilities", 2003, page 11 et seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

786 The summit declaration calls for measures in the fight against cyberterrorism: "Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists" For more information see: http://en.g8russia.ru/docs/17.html.

787 For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

788 The United Nations (UN) is an international organisation founded in 1945 that had 191 Member States in 2007.

789 A/RES/45/121 adopted by the UN General Assembly on 14 December 1990. The full text of the Resolution is available at: http://www.un.org/documents/ga/res/45/a45r121.htm

790 UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available

В 2000 году Генеральная Ассамблея ООН приняла резолюцию о борьбе с преступным использованием информационных технологий, которая демонстрирует ряд совпадений с планом действий из 10 пунктов, принятым Группой восьми в 1997 году[791]. В своей резолюции Генеральная Ассамблея определила ряд мер для предотвращения злоупотреблений информационными технологиями, в том числе:

> *Государства должны гарантировать принятие законов и практических мер по изоляции тех, кто по нормам уголовного права злоупотребляет информационными технологиям.*
>
> *Сотрудничество между правоохранительными органами в расследовании и судебном преследовании международных случаев преступного использования информационных технологий должны быть согласованы между всеми заинтересованными государствами.*
>
> *Сотрудники правоохранительных органов должны быть обучены и оснащены для борьбы с преступным использованием информационных технологий.*

В 2002 году Генеральная Ассамблея ООН приняла еще одну резолюцию о борьбе с преступным использованием информационных технологий[792]. В этой резолюции говорится о существующих международных подходах борьбы с киберпреступностью и освещаются различные решения.

> *Отмечая работу международных и региональных организаций по борьбе с высокотехнологичной преступностью, включая работу Совета Европы по разработке Конвенции о кибернетической преступности, а также работу этих организаций по содействию диалогу между правительствами, частным сектором о безопасности и доверии в киберпространстве,*
>
> *1 Призывает Государства-Члены при разработке национальных законов, политики и практики в деле борьбы с преступным использованием информационных технологий надлежащим образом учитывать работу и достижения Комиссии по предупреждению преступности и уголовному правосудию и других международных и региональных организаций.*
>
> *2 Отмечает значение мер, изложенных в ее Резолюции 55/63, и вновь призывает государства-члены учитывать их в своих усилиях по борьбе с преступным использованием информационных технологий.*
>
> *3 Постановляет отложить рассмотрение этого вопроса до выполнения работы, предусмотренной в плане действий Комиссии по предупреждению преступности и уголовному правосудию по борьбе с высокотехнологичной и компьютерной преступностью.*

В 2004 году в ООН создана рабочая группа, занимающаяся спамом, киберпреступностью и другими вопросами, связанными с интернетом, подтвердив интерес ООН к участию в международных дискуссиях по опасностям киберпреступности[793].

На 11-м Конгрессе ООН по предотвращению преступлений и уголовному правосудию, состоявшемся в Бангкоке, Тайланд, в 2005 году, была принята Декларация, которая подчеркнула необходимость гармонизации усилий по борьбе с киберпреступностью[794]. Среди них были следующие вопросы:

> *Мы подтверждаем важность реализации действующих документов и дальнейшей разработки национальных мер и международного сотрудничества в области уголовного правосудия, такие, как рассмотрение вопроса об усилении и расширении существующих мер, в частности, по противодействию киберпреступности, отмыванию денег и незаконному обороту культурных ценностей, а также об экстрадиции, взаимной правовой помощи, конфискации и возвращения доходов, полученных преступным путем.*

---

at http://www.uncjin.org/Documents/EighthCongress.html.

791 A/RES/55/63. The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

792 A/RES/56/121. The full text of the Resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

793 Regarding the Creation of the Working Group, see the UN press release, 21st of September 2004, available at: http://www.un.org/apps/news/story.asp?NewsID=11991&Cr=internet&Cr1=.

794 "Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice", available at: http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

Мы отмечаем, что нынешний период глобализации информационных технологии и быстрое развитие новых телекоммуникационных и сетевых компьютерных систем сопровождается злоупотреблением этими технологиями в преступных целях. Поэтому мы приветствуем усилия по расширению и дополнению существующего сотрудничества при проведении предварительного расследования и судебного преследования высокотехнологичных преступлений и преступлений с использованием компьютера, в том числе путем развития партнерских отношений с частным сектором. Мы признаем важный вклад Организации Объединенных Наций, региональных и других форумов в борьбу с киберпреступностью и предлагаем Комиссии по предупреждению преступности и уголовному правосудию, принимая во внимание этот опыт, рассмотреть возможность предоставления дополнительной помощи в этой области под эгидой ООН в партнерстве с другими организациями, занимающимися аналогичными вопросами.

Кроме того, ряд решений, резолюций и рекомендаций ООН касается вопросов, связанных с киберпреступностью. Важнейшими из них являются:

- Управление ООН по наркотикам и преступности (UNODC) Комиссии по предупреждению преступности и уголовному правосудию[795] приняло резолюцию об эффективной профилактике преступлений и уголовному правосудию по борьбе с сексуальной эксплуатацией детей[796].
- В 2004 году Экономический и социальный совет ООН[797] принял резолюцию о международном сотрудничестве в деле предотвращения, расследования, судебного преследования и наказания в преступлениях, связанных с мошенничеством, преступным неправомерным использованием и фальсификацией личных данных[798]. В 2007 году Совет принял резолюцию о международном сотрудничестве в деле предотвращения, расследования, судебного преследования и наказания экономического мошенничества и преступлений, связанных установлением идентичности[799]. Обе резолюции не решают всех проблем преступлений, связанных с интернетом[800], но хорошо применимы к подобным преступлениям.

  В 2004 году Совет принял резолюцию о законной торговле лекарствами через интернет, которая непосредственно касалась такого явления, как компьютерные преступления[801].

5.1.3 Международный союз электросвязи[802]

Международный союз электросвязи (МСЭ) в качестве специализированного учреждения в системе Организации Объединенных Наций играет ведущую роль в области стандартизации и развития электросвязи, а также в вопросах кибербезопасности. Среди прочей деятельности МСЭ является ведущей организацией Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), которая проходила в два этапа: в Женеве, Швейцария (2003 г.) и в Тунисе (2005 г.). Правительства, политики и эксперты всего мира обменялись идеями и опытом в отношении того, как лучше подойти к решению возникающих проблем, связанных с развитием глобального информационного общества, включая разработку совместимых стандартов и законов. Результаты встречи на высшем уровне, содержатся в *Женевской декларации*

795 The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up in 1991. It is a subsidiary body of the Economic and Social Council

796 CCPCJ Resolution 16/2 on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process within the development of the resolution and for an overview about different existing legal instruments see: Note by the Secretariat regarding Commission on Crime prevention and criminal justice responses to urban crime, including gang-related activities, and effective crime prevention and criminal justice responses to combat sexual exploitation of children, CN.15/2007/CRP.3, available at: http://www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative to the resolution see: http://www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

797 The United Nations Economic and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues. For more information see: http://www.un.org/ecosoc/.

798 ECOSOC Resolution 2004/26 International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: http://www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf

799 ECOSOC Resolution 2007/20 on international cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: http://www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf.

800 Regarding Internet-related ID-Theft, see above: Chapter 2.7.3 and below: Chapter 6.1.15.

801 ECOSOC Resolution 2004/42 on sale of internationally controlled licit drugs to individuals via the Internet, available at: http://www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

802 The International Telecommunication Union (ITU) with headquarter in Geneva was founded as International Telegraph Union in 1865. It is a specialised agency of the United Nations. The ITU has 191 Member States and more than 700 Sector Members and Associates. For more information see http://www.itu.int.

принципов, *Женевском плане действий*, *Тунисском обязательстве* и *Тунисской программе для информационного общества*.

Женевский план действий подчеркивает важность мер по борьбе с киберпреступностью[803]:

> ***C5 Укрепление доверия и безопасности при использовании ИКТ***
>
> ***12 Доверие и безопасность относятся к числу основных направлений развития информационного общества.***
>
> *b) Правительства в сотрудничестве с частным сектором должны предупреждать, выявлять и реагировать на киберпреступность и ненадлежащее использование ИКТ путем: разработки руководящих принципов, которые принимают во внимание продолжающиеся усилия в этих областях; рассмотрения законодательства, которое позволяет проводить эффективное расследование и уголовное преследование злоупотреблений; содействия эффективной взаимной помощи; укрепления институциональной поддержки на международном уровне для предотвращения, обнаружения и восстановления после таких инцидентов, а также содействия образованию и повышению осведомленности общественности.*

Проблема киберпреступности была также рассмотрена на второй части ВВУИО в Тунисе в 2005 году Тунисская программа для информационного общества[804] подчеркивает необходимость международного сотрудничества в борьбе с киберпреступностью и ссылается на действующие законодательные подходы, такие как Резолюции Генеральной Ассамблеи ООН и Конвенция Совета Европы о киберпреступности:

> ***40*** *Мы подчеркиваем важность уголовного преследования киберпреступности, в том числе киберпреступлений, совершенных в одной стране, но имеющих последствия в другой. Мы также подчеркиваем необходимость эффективных и действенных инструментов и мер на национальном и международном уровнях для содействия международному сотрудничеству, в частности, правоохранительным органам в сфере киберпреступности. Мы призываем правительства сотрудничать с другими заинтересованными сторонами в разработке необходимого законодательства для расследования и уголовного преследования киберпреступлений, помня об имеющейся основе, например резолюции Генеральной Ассамблеи ООН 55/63 и 56/121 "Борьба с преступным использованием информационных технологий" и региональные инициативы, в том числе, Конвенцию Совета Европы о киберпреступности, но не только.*

По итогам ВВУИО МСЭ было поручено взять на себя руководство по Направлению деятельности С5 по укреплению доверия и безопасности в области использования информационных и коммуникационных технологий[805]. На втором собрании по содействию реализации Направления деятельности С5 ВВУИО, состоявшемся в 2007 году, Генеральный секретарь МСЭ подчеркнул важность международного сотрудничества в борьбе с киберпреступностью и объявил о начале *Глобальной программы кибербезопасности МСЭ*[806]. Глобальная программа кибербезопасности имеет семь основных целей[807] и строится на пяти стратегических принципах[808], включающих разработку стратегии развития модели законодательства в сфере киберпреступности. Семь основных целей таковы:

> *1 Формирование стратегий разработки типового законодательства по борьбе с киберпреступностью, которое можно применять в глобальном масштабе и которое совместимо с действующими национальными и региональными законодательными актами.*
>
> *2 Формирование глобальных стратегий для создания надлежащих национальных и региональных организационных структур и политики в области борьбы с киберпреступностью.*

---

803 WSIS Geneva Plan of Action, 2003, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

804 WSIS Tunis Agenda for the Information Society, 2005, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

805 For more information on C5 Action Line see http://www.itu.int/wsis/c5/ and also the Meeting Report of the Second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: http://www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the Meetign Report of the Third Facilitation Meeting for WSIS Action Line C5, 2008, available at: http://www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.

806 For more information, see http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

807 http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

808 The five pillars are: Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, International Cooperation. For more information, see: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

3 Разработка стратегии для установления приемлемых на глобальном уровне минимальных критериев безопасности и схем санкционирования для аппаратных средств и программных приложений и систем.

4 Разработка стратегий для создания глобальной структуры для наблюдения, оповещения и реагирования на инциденты для обеспечения международной координации деятельности в рамках новых и существующих инициатив.

5 Разработка глобальных стратегий для создания и утверждения общей и универсальной системы цифровой идентификации, а также необходимых организационных структур в целях обеспечения признания цифровых удостоверений личности без учета географических границ.

6 Разработка глобальной стратегии в целях содействия созданию человеческого и институционального потенциала для увеличения знаний и ноу-хау в секторах и во всех вышеупомянутых областях.

7 Подготовка предложений по основе глобальной стратегии, основанной на участии многих заинтересованных сторон, в целях налаживания международного сотрудничества, диалога и координации деятельности во всех вышеупомянутых областях.

Для подготовки плана, относящегося к ГПК, была создана группа экспертов[809].

5.1.4 Совет Европы[810]

В 1976 году Совет Европы (CoE) подчеркнул международный характер компьютерных преступлений и обсудил эту тему на конференции по аспектам экономических преступлений. С тех пор эта тема остается в его повестке дня[811]. В 1985 г. Совет Европы утвердил комитет экспертов[812] для обсуждения правовых аспектов компьютерных преступлений[813]. В 1989 г. Европейский комитет по проблемам преступности одобрил "Доклад экспертов по компьютерным преступлениям"[814], проанализировав основные положения уголовного права, необходимые для борьбы с новыми формами электронных преступлений, в том числе компьютерным мошенничеством и подделкой. В 1989 г. Комитет министров принял рекомендацию[815], в которой особо подчеркнул международный характер компьютерной преступности:

Комитет министров в соответствии с положениями Статьи 15.b Устава Совета Европы считает, что целью Совета Европы является достижение большего единства между его членами.

Признавая важность адекватного и быстрого реагирования на новые задачи, связанные с компьютерной преступностью; учитывая, что компьютерные преступления часто имеют трансграничный характер; сознавая, что в результате необходима дальнейшая гармонизация законодательства и практики, а также для совершенствования международно-правовой сотрудничества, рекомендует правительствам Государств-Членов:

1 Принять во внимание при рассмотрении своих законодательств или при разработке новых законодательств доклад о компьютерной преступности, разработанный Европейским комитетом по проблемам преступности в части руководящих принципов для национальных законодательств.

2 Доклад Генерального секретаря Совета Европы в 1993 г. о любых изменениях в законодательстве, судебной практике и опыте международного правового сотрудничества в области компьютерных преступлений.

---

809 See: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

810 The Council of Europe, based in Strasbourg and founded in 1949, is an international organisation representing 47 member states in the European region. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organisation.

811 Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

812 The Expert Committee consisted of 15 experts, as well as observers from Canada, Japan, United States, the EEC, OECD and UN. Source: Nilsson in *Sieber*, "Information Technology Crime", Page 577.

813 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

814 *Nilsson* in Sieber, "Information Technology Crime", Page 576.

815 Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

В 1995 году Комитет министров принял другую рекомендацию по изучению проблем, возникающих в связи с транснациональными компьютерными преступлениями[816]. Руководство по разработке соответствующего законодательства приведено в приложении к этой рекомендации[817].

В 1996 году Европейский комитет по проблемам преступности (CDPC) принял решение о создании Комитета по борьбе с киберпреступностью[818]. Идея выхода за пределы принципов другой рекомендации и проекта Конвенции была представлена во время создания Комитета экспертов[819]. В период с 1997 г. по 2000 г. Комитет провел десять пленарных заседаний и пятнадцать совещаний открытой рабочей группы. Ассамблея приняла проект конвенции на второй части своей пленарной сессии в апреле 2001 года[820]. Окончательный проект конвенции был представлен на утверждение CDPC, а затем текст проекта конвенции был представлен на рассмотрение Комитета Министров для утверждения и открыт для подписания. Конвенция была открыта для подписания на церемонии подписания в Будапеште 23 ноября 2001 года, в ходе которой 30 стран подписали Конвенцию, включая четыре страны, не входящие в Совет Европы: Канада, США, Япония и ЮАР, которые принимали участие в переговорах. В апреле 2009 года 46 стран[821] подписали и 25 стран[822] ратифицировали[823] Конвенцию о киберпреступности. Такие страны, как Аргентина[824], Пакистан[825], Филиппины[826], Египет[827], Ботсвана[828] и Нигерия[829], уже разработали части своих законодательств в соответствие с Конвенцией. Хотя эти страны еще не подписали Конвенцию, они оказывают содействие гармонизации и стандартизации процесса, предполагаемого авторами Конвенции. В настоящее время Конвенция признана важнейшим международным инструментом в борьбе с киберпреступностью и поддержана различными международными организациями[830].

---

816 Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

817 The Guidelines deal with investigative instruments (e.g. Search and Seizure) as well as electronic evidence and international cooperation.

818 Decision CDPC/103/211196. The CDPC explained their decision by pointing out the international dimension of computer crimes: “By connecting to communication and information services, users create a kind of common space, called "cyber-space", which is used for legitimate purposes, but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities.”

819 Explanatory Report of the Convention on Cybercrime (185), No. 10.

820 The full text of the Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: http://www.coe.int.

821 Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

822 Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Serbia, Slovakia, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine, United States.

823 The need for a ratification is laid down in Article 36 of the Convention:

Article 36 – Signature and entry into force

1) This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2)This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

824 Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation, set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).

825 Draft Electronic Crime Act 2006

826 Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

827 Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

828 Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

829 Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

830 Interpol highlighted the importance of the Convention on Cybercrime in the Resolution of the 6th International Conference on Cyber Crime, Cairo: “That the Convention on Cyber Crime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages.“, available at: http://www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp; The 2005 WSIS Tunis Agenda points out: „We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on “Combating the criminal misuse of information technologies” and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime”, available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf; APEC called for economies to study the Convention on Cybercrime, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008,

За Конвенцией последовал первый дополнительный протокол к Конвенции о киберпреступности[831]. В ходе обсуждения текста конвенции выяснилось, что особенности уголовного преследования за расизм и распространение ксенофобных материалов является спорным вопросом[832]. Некоторые страны, которые имеют сильные позиции по защите права свободы самовыражения[833], выразили озабоченность, что если в Конвенцию будут включены положения, нарушающие свободу самовыражения, то они не смогут подписать Конвенцию[834]. Поэтому эти вопросы были включены в отдельный протокол. В октябре 2008 г. 20 стран[835] подписали и 13 стран[836] ратифицировали Дополнительный протокол.

В своем стремлении к совершенствованию защиты несовершеннолетних от сексуальной эксплуатации Совет Европы в 2007 г. представил новую Конвенцию[837]. В первый день, когда Конвенция о защите детей была открыта для подписания, ее подписали 23 государства[838]. Одной из главных целей Конвенции является гармонизация положений уголовного законодательства, направленных на защиту детей от сексуальной эксплуатации[839]. Для достижения этой цели Конвенция содержит положения уголовного законодательства. Помимо уголовной ответственности за сексуальное надругательство над детьми (Статья 18) Конвенция содержит положения, касающиеся обмена детской порнографией (Статья 20) и положения о сексуальных домогательствах к детям (Статья 23).

5.2 Региональные подходы

Наряду с международными организациями, которые ведут активную работу по всему миру, некоторые международные организации в конкретных регионах проявляют свою активность в вопросах, касающихся киберпреступности.

---

page 18, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; OAS called for an evaluation of the Convention while designing Cybercrime legislation, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 19, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

831 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

832 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime No. 4: "The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention."

833 Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq. , available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

834 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

835 Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine.

836 Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, France, Latvia, Lithuania, Norway, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine

837 Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

838 Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Irland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia, Turkey. Denmark, Iceland, Italy, Ukraine and the United Kingdom followed (July 2008).

839 For more details see *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

5.2.1 Европейский союз[840]

Европейский союз имеет ограниченные полномочия в отношении законодательства в области уголовного права[841]. Он обладает способностью гармонизировать национальное уголовное законодательство только в специальных областях, таких как защита финансовых интересов Европейского Союза и киберпреступность[842].

В 1999 году Европейский союз приступил к осуществлению инициативы "Электронная Европа", путем принятия Европейской комиссией связи проекта "Электронная Европа – информационное общество для всех"[843]. В 2000 году Совет Европы принял всеобъемлющий "План действий Электронная Европа" и призвал к его реализации до конца 2002 года.

В 2001 году Европейская комиссия опубликовала сообщение на тему "Создание безопасного информационного общества, повышение безопасности информационных инфраструктур и борьба с компьютерной преступностью"[844]. В этом сообщении Комиссия проанализировала и изучила проблему киберпреступности и указала на необходимость принятия эффективных мер для борьбы с угрозой обеспечения целостности, доступности и надежности информационных систем и сетей.

> *Информационные и коммуникационные инфраструктуры стали важной частью нашей экономики. К сожалению, эти инфраструктуры из-за собственной уязвимости открывают новые возможности для преступной деятельности. Эти преступные действия могут принимать самые разнообразные формы и могут пересекать множество границ. Хотя по ряду причин нет надежных статистических данных, существует мало сомнений в том, что эти преступления представляют собой угрозу для промышленных инвестиций и активов, а также безопасности и доверия в информационном обществе. Некоторые последние примеры отказа в оказании услуг и вирусные атаки нанесли серьезный финансовый ущерб.*
>
> *Существует возможность для действий в плане предотвращения преступной деятельности путем повышения безопасности информационной инфраструктуры и обеспечения того, чтобы правоохранительные органы имели соответствующие средства для ответных действий, при полном уважении основных прав человека*[845].
>
> *Комиссия, приняв участие в дискуссиях и Совета Европы, и Группы восьми, признает сложности и трудности, связанные с вопросами процессуального права. Однако эффективное сотрудничество внутри ЕС по борьбе с киберпреступностью является важным элементом более безопасного информационного общества и создания зоны свободы, безопасности и правосудия*[846].
>
> *Комиссия будет выдвигать законодательные предложения в соответствии с разделом VI TEU:*
>
> *[...] к дальнейшему приближению существующего уголовного права к области высокотехнологичной преступности. К ним относятся преступления, связанные с хакерскими атаками и отказами в доступе. Комиссия будет также изучать возможности для действий, направленных против расизма и ксенофобии в интернете, с тем чтобы предложить в соответствии с разделом VI TEU, охватывающим*

---

840 The European Union is a supranational and intergovernmental union of today 27 member states from the European continent.

841 *Satzger*, International and European Criminal Law, Page 84; *Kapteyn/VerLooren van Themaat*, Introduction to the Law of the European Communities, Page 1395.

842 Regarding the Cybercrime legislation in respect of Computer and Network Misuse in EU Countries see: *Baleri/Somers/Robinson/Graux/Dumontier*, Handbook of Legal Procedures of Computer Network Misuse in EU Countries, 2006.

843 Communication of 8 December 1999 on a Commission initiative for the special European Council of Lisbon, 23 and 24 March 2000 - *e*Europe - An information society for all – COM 1999, 687.

844 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime26.1.2001, COM(2000) 890.

845 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, Page 23.

846 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, Page 23.

офлайновую и онлайновую расистскую и ксенофобскую деятельность. Наконец, проблема незаконного оборота наркотиков в интернете также будет рассмотрена[847].

Комиссия будет и впредь играть активную роль в обеспечении координации между Государствами-Членами в других международных форумах по борьбе с киберпреступностью, таких как Совет Европы и Группа восьми. Инициативы Комиссии на уровне ЕС будут в полной мере учитывать прогресс других международных форумов, стремясь добиться сближения в рамках ЕС[848].

Кроме того, в 2001 году Комиссия опубликовала коммюнике "Сеть и информационная безопасность[849]", в котором были проанализированы проблемы безопасности сети и разработан стратегический план действий в этой области.

В обоих этих коммюнике Комиссии подчеркивалась необходимость сближения существующего уголовного права стран Европейского союза, особенно в связи с атаками на информационные системы. Гармонизация основного уголовного права стран Европейского союза в области борьбы с киберпреступностью признана одним из ключевых элементов всех инициатив на уровне ЕС[850]. Следуя этой стратегии, в 2002 году Комиссия[851] представила предложение по "Рамочному решению по атакам на информационные системы". Предложение Комиссии было частично изменено и в итоге принято Советом[852].

Рамочное решение учитывает Конвенцию Совета Европы о киберпреступности[853], но сосредоточено на гармонизации основных положений уголовного законодательства, которые предназначены для защиты элементов инфраструктуры.

Статья 2 – Противозаконный доступ к информационным системам

1 Каждое Государство-Участник принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать преднамеренный неправомерный доступ к компьютерной системе в целом или любой ее части как уголовное преступление, по крайней мере, для случаев, которые не являются незначительными.

2 Каждое Государство-Участник может принять решение о том, что деяния, указанные в пункте 1, инкриминируются только в случае, если преступление совершено с нарушением мер безопасности, и карается эффективным, пропорциональным и оказывающим сдерживающее воздействие уголовным наказанием.

Статья 3 – Противозаконное воздействие на функционирование системы

Каждое Чосударство-Член принимает необходимые меры, чтобы квалифицировать умышленное создание серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных как уголовное преступление, совершенное неправомерно, по крайней мере, для случаев, которые не являются незначительными.

---

847 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, Page 31.

848 Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, Page 32.

849 "Network and Information Security" A European Policy approach - adopted 6 June 2001.

850 For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

851 Proposal of the Commission for a Council Framework Decision on attacks against information systems – 19. April 2002 – COM (2002) 173. The legal basis for the Framework Decision, indicated in the preamble of the proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See: *Gercke*, Framework Decision on Attacks against Information Systems, CR 2005, 468 et seq.

852 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

853 See the explanation of the Framework Decision in the Proposal For A Council Framework Decision on combating serious attacks against information systems, No. 1.6:
"Legislative action at the level of the European Union also needs to take into account developments in other international fora. In the context of approximation of substantive criminal law on attacks against information systems, the Council of Europe (C.o.E.) is currently the most far-advanced. The Council of Europe started preparing an international Convention on cyber-crime in February 1997, and is expected to complete this task by the end of 2001. The draft Convention seeks to approximate a range of criminal offences including offences against the confidentiality, integrity and availability of computer systems and data. This Framework Decision is intended to be consistent with the approach adopted in the draft Council of Europe Convention for these offences."

Статья 4 – Противозаконное воздействие на данные

Каждое Государство-Член принимает необходимые меры, чтобы квалифицировать умышленное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных информационных систем как уголовное преступление, совершенное неправомерно, по крайней мере, для случаев, которые не являются незначительными.

В 2005 году суд Европейского Сообщества объявил незаконным[854] Рамочное решение Совета по вопросам охраны окружающей среды посредством уголовного законодательства[855]. Этим решением суд уточнил распределение полномочий между первой и третьей опорами в отношении положений уголовного права. Суд решил, что Рамочное решение по защите окружающей среды посредством уголовного законодательства, будучи неделимым, нарушает Статью 47 ЕС, поскольку оно посягает на полномочия, которые дает Евросовету в сообществе Статья 175 ЕС[856]. В сообщении о решении суда[857] Комиссия выразила:

"С точки зрения существа предмета, в дополнение к охране окружающей среды аргументация Суда может быть применена ко всем правам и свободам сообщества, которые включают в себя законодательные акты, с тем чтобы уголовное наказание могло обеспечить их эффективность."

Комиссия заявила, что в результате решения суда несколько положений Рамочного решения, касающиеся уголовного права, становятся полностью или частично не верными, так как все эти положения или некоторые из них были приняты на неправильной законодательной базе. Рамочное решение об атаках на информационные системы прямо упоминается в поправке к коммюнике.

Аспекты уголовно-процессуального права, прежде всего, согласование документов, необходимых для расследования и судебного преследования киберпреступности, не были включены в Рамочное решение. Тем не менее, в 2005 году Комиссия подготовила предложение по Директиве Европейского союза по вопросу сохранения данных. Всего через три месяца после представления в Европейском парламенте Совет принял это предложение[858]. Ключевым элементом этой Директивы является обязанность поставщика услуг интернета хранить определенные данные о трафике, которые необходимы для идентификации преступников в киберпространстве:

Статья 3 – Обязательство хранить данные

1 В порядке отступления от положений статей 5, 6 и 9 Директивы 2002/58/ЕС, Государства-Участники должны принять меры для обеспечения того, чтобы хранить данные, указанные в Статье 5 настоящей Директивы, в такой степени, чтобы эти данные могли быть сформированы или обработаны поставщиками услуг электронной связи общего пользования или поставщиками сетей общего пользования, в рамках их юрисдикции в процессе предоставления указанных услуг связи.

2 Обязательство хранить данные, предусмотренное пунктом 1, включает в себя сохранение данных, указанных в Статье 5, относящихся к неудачной попытке вызова, когда эти данные сформированы, обработаны и сохранены (в случае телефонных данных) или записаны (в случае данных интернета) поставщиками услуг электронной связи общего пользования или

---

854 Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.

855 Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03.

856 "It follows from the foregoing that, on account of both their aim and their content, Articles 1 to 7 of the framework decision have as their main purpose the protection of the environment and they could have been properly adopted on the basis of Article 175 EC. That finding is not called into question by the fact that Articles 135 EC and 280(4) EC reserve to the Member States, in the spheres of customs cooperation and the protection of the Community's financial interests respectively, the application of national criminal law and the administration of justice. It is not possible to infer from those provisions that, for the purposes of the implementation of environmental policy, any harmonisation of criminal law, even as limited as that resulting from the framework decision, must be ruled out even where it is necessary in order to ensure the effectiveness of Community law. In those circumstances, the entire framework decision, being indivisible, infringes Article 47 EU as it encroaches on the powers which Article 175 EC confers on the Community."

857 Communication From The Commission To The European Parliament And The Council on the implications of the Court's judgment of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583.

858 2005/0182/COD

поставщиками сетей общего пользования, в рамках юрисдикции Государства-Участника, затронутого в процессе в случае предоставления указанных услуг связи. Данная Директива не требует сохранения данных при попытке вызова, когда соединение не было установлено.

Тот факт, что эта Директива касается основной информации о любом сообщении в интернете, привел к интенсивной критике со стороны правозащитных организаций и может привести к пересмотру Директивы и ее применения в конституционных судах[859].

В 2007 году Комиссия опубликовала сообщение в отношении общей политики по борьбе с киберпреступностью[860]. В сообщении обобщена существующая ситуация и подчеркнута важность того, чтобы конвенция Совета Европы о киберпреступности стала основным международным инструментом по борьбе с киберпреступностью. Кроме того, в сообщении указаны вопросы, которым будет посвящена будущая деятельность Комиссии. К ним относятся:

- укрепление международного сотрудничества в борьбе с киберпреступностью;
- улучшение координации финансовой поддержки обучения;
- организация встречи экспертов правоохранительных органов;
- укрепление диалога с промышленностью;
- наблюдение за развитием угроз со стороны киберпреступности с целью оценки потребности в дальнейших работах над законодательством.

В 2008 году Европейский союз приступил к обсуждению проекта поправок к Рамочному решению о борьбе с терроризмом[861]. Во введении к проекту поправки Европейский союз подчеркивает, что существующие правовые рамки считают преступлением пособничество, подстрекательство или разжигание, но не относят к криминалу распространение террористических навыков через интернет[862]. Этой поправкой Европейский союз стремится принять меры по сокращению разрыва и приведению законодательства на всей территории Евросоюза к Конвенции Совета Европы о предупреждении терроризма.

Статья 3 – Преступления, связанные с террористической деятельностью

1 В целях Рамочного решения:

a) "публичное подстрекательство к совершению террористического преступления" означает распространение или иное предоставление в распоряжение обращения к общественности с намерением подстрекать к совершению одного из деяний, перечисленных в Статье 1(1a) до h)), где такое поведение, существует или нет прямой призыв к террористическому нападению, вызывает опасения, что одно или несколько таких нападений могут быть совершены;

b) "наем для терроризма" означает подстрекательство другого лица к совершению одного из деяний, перечисленных в Статье 1(1), или в Статье 2(2);

c) "подготовка кадров для терроризма" означает проведение обучения для изготовления или применения взрывчатых веществ, огнестрельного или другого оружия, ядовитых или опасных веществ или других специальных методов и технологий с целью совершения одного из деяний, перечисленных в Статье 1(1), сознавая, что навыки должны быть использованы для этих целей.

2 Каждое Государство-Участник должно принять необходимые меры для обеспечения того, что преступления относятся к террористическим, если содержат следующие преднамеренные действия:

a) публичное подстрекательство к совершению террористического преступления;

---

859 *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, 286.

860 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267. For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

861 Draft Proposal for a Council Framework Decision amending Framework Decision 2002/475/JHA on combating terrorism, COM(2007) 650.

862 "Article 4 of the Framework Decision on combating terrorism states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States. Article 2 of the same instrument requires Member States to hold those directing a terrorist group or participating in its activities criminally liable. However, these provisions do not explicitly cover the dissemination of terrorist propaganda and terrorist expertise, in particular through the Internet."

b) наем для терроризма;

c) подготовка кадров для терроризма;

d) кража при отягчающих обстоятельствах с целью совершения одного из деяний, перечисленных в Статье 1(1);

e) вымогательство с целью совершения одного из деяний, перечисленных в Статье 1(1);

f) составление ложных административных документов с целью совершения одного из деяний, перечисленных в Статье 1(1a) до h)) и Статье 2(2b).

3 Для деяний, которые наказуемы, как указано в пункте 2, не обязательно, что террористическое преступление было реально совершено".

На основании Статьи 3, пункт 1 c)[863] Рамочного решения, Государства-Участники, к примеру, вынуждены вводить уголовную ответственность за публикацию инструкций по использованию взрывчатых веществ, если известно, что эта информация предназначена для использования в террористических целях. Необходимость доказательства того, что информация весьма вероятно намеренно должны быть использована для террористических целей, ограничивает применение этого положения, в связи с тем, что большинство инструкций по использования оружия, имеющихся в интернете, как и их публикация, непосредственно не связаны с террористическими атаками. Поскольку большая часть оружия и взрывчатых веществ может быть использована для совершения как "обычных" преступлений, так и для террористических преступлений (двойного назначения), то сама информация вряд ли может быть использована как доказательство, что человеку, который ее обнародовал, было известно, каким образом такая информация будет использована впоследствии. Поэтому необходимо обращать внимание на содержание публикаций, например на веб-сайте террористической организации.

5.2.2 Организация экономического сотрудничества и развития[864]

В 1983 году Организация экономического сотрудничества и развития (ОЭСР) провела исследование по вопросу о возможности международной гармонизации уголовного законодательства в целях решения проблемы компьютерной преступности[865]. В 1985 году она опубликовала доклад, в котором было проанализировано действующее законодательство и внесены предложения по борьбе с киберпреступностью[866]. Она рекомендовала минимальный перечень преступлений, для которых страны должны рассмотреть вопрос уголовной ответственности, например, компьютерное мошенничество, подделка, произведенная при помощи компьютера, изменение компьютерных программ и данных, а также перехват сообщений. В 1990 году Комитет по информационной, компьютерной и коммуникационной политике создал группу экспертов по разработке свода руководящих принципов по информационной безопасности, который был составлен к 1992 году и затем принят Советом ОЭСР[867]. Эти руководящие принципы включают среди прочего вопросы о санкциях:

Санкции за неправомерное использование информационных систем являются важным средством в деле защиты интересов тех информационных систем, которые пострадали в результате атаки на доступность, конфиденциальность и целостность информационных систем и их компонентов. Примерами таких атак может быть повреждение или сбой информационных систем посредством введения вирусов и червей, изменения данных, незаконного доступа к данным, компьютерного мошенничества или подлога, а также несанкционированного воспроизведения компьютерных программ. Для борьбы с такими опасностями страны выбирают различные описание и реагирование на преступные действия. Растет международное согласие относительно основ компьютерных преступлений, которые должны быть охвачены национальным уголовным законодательством. В течение последних двух десятилетий это нашло свое отражение в развитие законодательства по компьютерной преступности и защите данных в странах – членах ОЭСР и в работе ОЭСР и других международных органов по вопросам

---

[863] "training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.

[864] The Organisation for Economic Co-operation and Development was founded 1961. It has 30 member states and is based in Paris. For more information see: http://www.oecd.org.

[865] *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[866] OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.

[867] In 1992 the Council of the OECD adopted the Recommendation concerning Guidelines for the Security of Information Systems. The 24 OECD Member countries adopted the Guidelines later.

законодательства по борьбе с компьютерной преступностью […[. Национальное законодательство должно периодически пересматриваться, чтобы адекватно отвечать опасностям, связанным с использованием информационных систем.

После рассмотрения руководящих принципов в 1997 году в 2001 году Комитет по информационной, компьютерной и коммуникационной политике создал вторую группу экспертов для обновления руководящих принципов. В 2002 году новая версия руководящих принципов "Руководящие принципы ОЭСР по обеспечению безопасности информационных систем и сетей: к культуре безопасности", была принята в качестве Рекомендации Совета ОЭСР[868]. Эти руководящие принципы содержат девять взаимодополняющих принципов:

1) Осведомленность

Участники должны быть осведомлены о необходимости обеспечения безопасности информационных систем и сетей, а также о том, что они могут сделать для повышения безопасности.

2) Ответственность

Все участники несут ответственность за безопасность информационных систем и сетей.

3) Реакция

Участники должны действовать на своевременной и коллективной основе в целях предотвращения, обнаружения и реагирования на инциденты в области безопасности.

4) Этика

Участники должны уважать законные интересы других лиц.

5) Демократия

Безопасность информационных систем и сетей должна быть совместима с основными ценностями демократического общества.

6) Оценка риска

Участники должны производить оценку риска.

7) Безопасный дизайн и реализация

Участники должны рассматривать соображения безопасности в качестве одного из основных элементов информационных систем и сетей.

8) Управление безопасностью

Участники должны принять комплексный подход к управлению безопасностью.

9) Переоценка

Участникам следует пересмотреть и переоценить безопасность информационных систем и сетей, а также внести соответствующие изменения в политику, практику, меры и процедуры безопасности.

В 2005 году ОЭСР опубликовала доклад, в котором проанализировано влияние спама на развивающиеся страны[869]. Доклад показал, что в связи с более ограниченными и более дорогими ресурсами в развивающихся странах спам является гораздо более серьезной проблемой, чем в западных странах[870].

После получения запроса от подразделения стратегического планирования канцелярии Генерального секретаря ООН подготовить примерное сравнение национальных законодательных решений в отношении использования интернета в террористических целях, в 2007 году ОЭСР опубликовала доклад о законодательных решениях в отношении "Кибертерроризма" в рамках внутреннего законодательства отдельных государств[871].

---

[868] Adopted by the OECD Council at its 1037th Session on 25 July 2002. The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, available at: http://www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html

[869] Spam Issue in Developing Countries. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

[870] See Spam Issue in Developing Countries, Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

[871] The report is available at: http://www.legislationline.org/upload/ lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.

5.2.3 Азиатско-тихоокеанское экономическое сотрудничество[872]

В 2002 году лидеры стран Азиатско-тихоокеанского экономического сотрудничества (АТЭС) выпустили "Заявление по борьбе с терроризмом и обеспечению роста", чтобы принять всеобъемлющие законы, связанные с киберпреступностью и разработать национальные средства расследований киберпреступлений[873]. Они решили:

- Приложить усилия к тому, чтобы к октябрю 2003 года принять всеобъемлющий свод законов, касающихся кибербезопасности и киберпреступности, которые согласуются с положениями международно-правовых документов, в том числе с положениями Резолюции 55/63 (2000 г.) Генеральной Ассамблеи ООН и Конвенции о киберпреступности (2001 г.).
- К октябрю 2003 года определить национальные подразделения по киберпреступности и контактные центры международной высокотехнологичной помощи и создать такие средства, какими они еще не обладают.
- Создать учреждения для обмена информацией об угрозе и оценке уязвимости, например, группы реагирования на компьютерные происшествия.

Лидеры стан АТЭС призвали к более тесному сотрудничеству должностных лиц, участвующих в борьбе с киберпреступностью[874]. В 2005 г. АТЭС была организована конференция по законодательству в сфере киберпреступности[875]. Основными целями конференции были:

- содействие разработке комплексной правовой базы для борьбы с киберпреступностью и содействия кибербезопасности;
- оказание помощи правоохранительным органам для реагирования на современные проблемы, связанные с технологическим прогрессом;
- содействие сотрудничеству между органами, осуществляющими расследование киберпреступлений по всему региону.

Рабочая группа по электросвязи и информации АТЭС[876] активно участвовала в разработке подходов АТЭС для повышения кибербезопасности[877]. В 2002 году была принята Стратегия кибербезопасности АТЭС[878]. Рабочая группа выразила свою позицию в отношении законодательства в сфере киберпреступности, ссылаясь на существующие международные подходы ООН и Совета Европы[879]. В Декларации, принятой в 2008 году на Встрече министров связи и информации стран АТЭС в Бангкоке, Таиланд, была подчеркнута важность продолжения сотрудничества в борьбе с киберпреступностью[880].

---

872 The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties that has 21 members.

873 APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico 26 October 2002. Regarding the national legislation on Cybercrime in the Asian-Pacific Region see: Urbas, Cybercrime Legislation in the Asia-Pacific Region, 2001, available at: http://www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf; See in this regards as well: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

874 "*We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime*." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

875 Cybercrime Legislation and Enforcement Capacity Building Project – 3rd Conference of Experts and Training Seminar, APEC Telecommunications and Information Working Group, 32nd Meeting, 5-9 September 2005, Seoul, Korea.

876 "Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws."

877 The APEC Telecommunications and Information Working Group was founded in 1990. It aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing information policies. For more information see: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

878 For more information see: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.MediaLibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/som/mtg/2002/word.Par.0204.File.v1.1

879 See: http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

880 The Ministers stated in the declaration "their call for continued collaboration and sharing of information and experience between member economies to support a safe and trusted ICT environment including effective responses to ensure security against cyber threats, malicious attacks and spam." For more information see:

5.2.4 Содружество

Принимая во внимание растущее значение борьбы с киберпреступностью, министры юстиции Содружества решили организовать группу экспертов для разработки правовых норм по борьбе с киберпреступности на основе Конвенции Совета Европы о киберпреступности[881]. На этот подход к гармонизации законодательства в рамках Содружества и международного сотрудничества, наряду с другими вопросами, повлиял тот факт, что без подобного подхода потребуется более 1272 двусторонних переговоров в рамках Содружества о международном сотрудничестве в этом вопросе[882]. Группа экспертов представила свой доклад и рекомендации в марте 2002 года[883]. Позже в 2002 году был представлен Проект типового закона о компьютерах и компьютерных преступлениях[884]. Необходимость в четких инструкциях, а также признание группой экспертов Конвенции о киберпреступности в качестве международного стандарта, ставит типовой закон в один ряд со стандартами, определенными Конвенцией о киберпреступности.

5.2.5 Лига арабских государств и Совет сотрудничества стран Залива[885]

Многие страны арабского региона уже предприняли национальные меры и утвердили подходы для борьбы с киберпреступностью или находятся в процессе разработки законодательства[886]. Среди таких стран: Пакистан[887], Египет[888] и Объединенные Арабские Эмираты[889] (ОАЭ). Совет сотрудничества стран Залива (ССЗ[890]) на конференции в 2007 году рекомендовал странам ССЗ искать совместный подход, который учитывал бы международные стандарты[891].

5.2.6 Организация американских государств[892]

С 1999 года Организация американских государств (ОАГ) активно рассматривает вопрос о киберпреступности в этом регионе. Среди прочего, в рамках мандата и сферы деятельности REMJA

---

http://www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

881 See “Model Law on Computer and Computer Related Crime”, LMM(02)17, Background information.

882 *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.

883 See: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

884 “Model Law on Computer and Computer Related Crime”, LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

885 The League of Arab States is a regional organisation with currently 22 members.

886 See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

887 Draft Electronic Crime Act 2006

888 Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

889 Law No.2 of 2006, enacted in February 2006.

890 Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and the UAE

891 Non official transation of the Recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18th of June 2007, Abu Dhabi:

1) Calling for the adoption of a treaty by the Gulf Cooperation Council (GCC) countries, inspired by the Council of Europe Cybercrime convention, to be expanded later to all Arab Countries.
2) Calling all GCC countries to adopt laws combating Cybercrime inspired by the model of the UAE Cybercrime Law.
3) Calling for the adoption of laws in relation to procedural matters such as seizure, inspection and other investigation procedures for such special type of crimes.
5) Providing trainings to inspection and law enforcement officials on dealing with such crimes.
6) Providing sufficient number of experts highly qualified in new technologies and Cybercrime particularly in regard to proofs and collecting evidence.
7) Recourse to the Council of Europe’s expertise in regard to Combating Cybercrime particularly in regard to studies and other services which would contribute in the elaboration and development of local countries legislation in GCC countries.
8) Harmonization of the legislations in Arab and particularly GCC countries in regard to basic principles in combating this type of crimes on both procedural and substantive level.
9) Increasing cooperation between Public and Private sectors in the intent of raising awareness and exchange of information in the Cybercrime combating field.

892 The Organisation of American States is an international organisation with 34 active Member States. For more information see: http://www.oas.org/documents/eng/memberstates.asp.

организация провела ряд встреч министров юстиции и министров или генеральных прокуроров стран Северной и Южной Америки[893].

В 1999 году REMJA рекомендовала создать межправительственную группу экспертов по киберпреступности. Группе экспертов было поручено:

- провести анализ преступной деятельности, целью которой являются компьютеры и информация, или в которых используются компьютеры в качестве средства совершения преступления;
- провести анализ национального законодательства, политики и практики в отношении такой деятельности;
- определить национальные и международные организации с соответствующим опытом;
- определить механизмы сотрудничества в рамках межамериканской системы по борьбе с киберпреступностью.

В 2000 году министры юстиции и министры или генеральные прокуроры стран американского континента рассмотрели тему киберпреступности и согласовали ряд рекомендаций[894]. Эти рекомендации были повторены на встрече в 2003 году[895] и включали следующее:

- Поддержать рассмотрение рекомендаций, сделанных Группой правительственных экспертов на своем первом заседании в качестве REMJA, как вклад в развитие межамериканской стратегии по борьбе с угрозами кибербезопасности, о которых говорится в резолюции Генеральной ассамблеи ОАГ AG/RES. 1939 /XXXIII-O/03), и обратиться к группе через своего представителя для продолжения оказания поддержки в подготовке стратегии.
- Государства – Члены экспертной группы должны рассмотреть механизмы, способствующие широкому и эффективному сотрудничеству между ними для борьбы с киберпреступностью, и провести, когда это возможно, разработку технической и правовой возможности присоединения к сетям в режиме 24/7, установленным Группой восьми для оказания помощи в расследовании киберпреступлений.
- Государства-Члены должны оценить целесообразность реализации принципов, закрепленных в Конвенции Совета Европы о киберпреступности 2001 года, и рассмотреть возможность присоединения к этой Конвенции.
- Государства-Члены должны провести обзор и, при необходимости, обновить структуру и работу внутренних органов или учреждений, отвечающих за обеспечение соблюдения законов, с тем чтобы адаптироваться к изменению характера киберпреступности, в том числе пересмотреть взаимоотношения между организациями, которые занимаются борьбой с киберпреступностью, и организациями, которые предоставляют традиционную полицейскую или правовую помощь.

Четвертая встреча министров юстиции и министров или генеральных прокуроров стран американского континента рекомендовала заново собрать Группу правительственных экспертов[896] по киберпреступности в рамках деятельности рабочей группы ОАГ для разработки дальнейших рекомендаций REMJA и потребовало:

---

[893] For more information see http://www.oas.org/juridico/english/cyber.htm and the Final report of the Fifth Meeting of REMJA, which contains the full list of reports, results of the plenary session and conclusions and recommendations at: http://www.oas.org/juridico/english/ministry_of_justice_v.htm.

[894] The full list of recommendations from the 2000 meeting is available at: http://www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber; The full list of recommendations from the 2003 meeting is available at: http://www.oas.org/juridico/english/ministry_of_justice_v.htm.

[895] The full list of recommendations is available at: http://www.oas.org/juridico/english/ministry_of_justice_v.htm

[896] The OAS' General Secretariat through the Office of Legal Cooperation of the Department of International Legal Affairs serves as the Technical Secretariat to this Group of Experts, pursuant to the resolutions of the OAS General Assembly. More information on the Office of Legal Cooperation is available at: http://www.oas.org/dil/department_office_legal_cooperation.htm.

- дополнить меры по осуществлению рекомендаций, подготовленные этой группой и утвержденные REMJA-III;
- рассмотреть вопрос о подготовке соответствующих межамериканских правовых документов и типовых законов в целях укрепления сотрудничества стран Западного полушария в борьбе с киберпреступностью, с учетом стандартов, относящихся к частной жизни, защите информации, процедурных аспектов и предупреждения преступности.

Министры юстиции и министры или генеральные прокуроры стран американского континента (REMJA) провели на сегодняшний день семь встреч[897]. Последние встречи были проведены в Вашингтоне, округ Колумбия, США, в апреле 2006 года и апреле 2008 года. Среди рекомендаций, представленных на встрече 2006 года, были следующие[898]:

- продолжить укреплять сотрудничество с Советом Европы, с тем чтобы Государства – Члены ОАГ могли рассмотреть вопрос о применении принципов Конвенции Совета Европы о киберпреступности[899]. Кроме того, продолжить укреплять механизмы обмена информацией и сотрудничества с другими международными организациями и учреждениями в области киберпреступности, такими как Организация Объединенных Наций, Европейский союз, Форум Азиатско-Тихоокеанского экономического сотрудничества, ОЭСР, Группа восьми, Содружество, а также Интерпол, для того чтобы Государства – Члены ОАГ воспользовались прогрессом в этих форумах;
- Государствам-Членам создать специальные подразделения для расследования киберпреступлений, а также определить органы, которые будут работать в качестве контактных в этом вопросе, и ускорять обмен информацией и получение доказательств. Кроме того, укреплять сотрудничество по борьбе с киберпреступностью среди государственных органов, поставщиков услуг интернета и других организаций частного сектора, предоставляющих услуги передачи данных.

Эти рекомендации были повторены на совещании 2008 года, где было отмечено[900]:

- что, с учетом рекомендаций Группы правительственных экспертов, принятых на предыдущих встречах REMJA, государствам, присоединившемся к Конвенции, необходимо рассмотреть вопрос о применении принципов Конвенции Совета Европы о киберпреступности и принять правовые и иные меры, необходимые для ее осуществления. Аналогичное в этой связи техническое сотрудничество с Советом Европы и впредь будет проводиться под эгидой Генерального секретаря ОАГ через Секретариат по правовым вопросам. Кроме того, продолжить предпринимать усилия с целью расширения обмена информацией и сотрудничества с другими международными организациями и учреждениями в области киберпреступности, так чтобы Государства – Члены ОАГ могли воспользоваться преимуществами достижений этих форумов.
- что Секретариат межамериканского комитета по борьбе с терроризмом (CICTE), Межамериканская комиссия электросвязи (CITEL) и рабочая группа по киберпреступности должны продолжить развивать постоянное сотрудничество и координацию действий в целях обеспечения реализации Глобальной

[897] The Conclusions and Recommendation of the Meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas and Cyber Crime are available at: http://www.oas.org/juridico/english/cyber_meet.htm.

[898] In addition the Working Group of Governmental Experts on cybercrime recommended that training be provided in the management of electronic evidence and that a training program be developed to facilitate states link-up to the 24 hour/7 day emergency network established by the G-8 to help conduct cyber-crime investigations. Pursuant to such recommendation, three OAS Regional Technical Workshops were held during 2006 and 2007, with the first being offered by Brazil and the United States, and the second and third offered by the United States. The List of Technical Workshops is available at: http://www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

[899] In the meantime the OAS has established joint collaboration with the Council of Europe and attended and participated in the 2007 Octopus Interface Conference on Cooperation against cybercrime. See: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp

[900] Conclusions and Recommendations of REMJA-VII, 2008, available at: http://www.oas.org/juridico/english/cybVII_CR.pdf

межамериканской стратегии о кибербезопасности, утвержденной резолюцией AG/RES. 2004 (XXXIV-O/04) Генеральной ассамблеи ОАГ.

5.3 Научные подходы

Хорошо известный пример научного подхода к разработке правовой основы для решения проблемы киберпреступности на глобальном уровне – это Проект Стэнфордской Международной Конвенции (CISAC[901]). Эта Конвенция была разработана по итогам конференции, проведенной в Стэнфордском университете Соединенных Штатов в 1999 году[902]. Сравнение с Конвенцией Совета Европы о киберпреступности[903], которая была разработана примерно в то же время, выявляет ряд совпадений. Оба документа охватывают аспекты материального уголовного права, процессуального права и международного сотрудничества. Главным различием является тот факт, что преступления и процессуальные документы, разработанные в Проекте Стэнфордской Конвенции, применяются только в связи с атаками на информационную инфраструктуру и террористическими нападениями, в то время как инструменты, связанные с процессуальным правом и международным сотрудничеством, упомянутые в Конвенции о киберпреступности, могут также применяться и по отношению к традиционным преступлениям[904].

5.4 Взаимосвязь между различными международными и законодательными подходами

Успех отдельных стандартов в части технических протоколов приводит к вопросу о том, как можно избежать конфликтов между различными международными подходами[905]. В настоящее время Конвенция о киберпреступности является главной действующей международной основой, которая охватывает все существенные аспекты, такие как киберпреступность, но также рассматривает и другие деяния. Второй международный подход в настоящее время предпринят Международным союзом электросвязи[906]. По итогам Всемирной встречи на высшем уровне по вопросам информационного общества, МСЭ назначен содействующей организацией для так называемого Направления деятельности С5 ВВУИО. Как определено на женевском этапе встречи ВВУИО в 2003 году, Направление деятельности С5 включает укрепление доверия и безопасности при использовании ИКТ[907]. На втором собрании по содействию реализации Направления деятельности С5, Генеральный секретарь МСЭ подчеркнул важность международного сотрудничества в борьбе с киберпреступностью. За этим последовал доклад о разработке в МСЭ Глобальной

---

[901] *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf.

[902] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[903] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention see below: Chapter 6.1.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq*.; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et. seqq; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: http://www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol 95, No.4, 2001, page 889 *et seq*.

[904] Regarding the application of Art. 23 et seq. with regard to tradition crimes see: Explanatory Report to the Convention on Cybercrime, No. 243.

[905] For details see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 et seq.

[906] The International Telecommunication Union (ITU) with headquarter in Geneva was founded as International Telegraph Union in 1865. It is a specialised agency of the United Nations. The ITU has 191 Member States and more than 700 Sector Members and Associates.

[907] For more information on the C5 Action Line see Meeting Report of 2nd Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/meetingreport.pdf.

программы кибербезопасности[908]. Глобальная программа кибербезопасности МСЭ (ГПК) преследует семь основных целей[909]. Одной из целей является формирование стратегий для разработки типового законодательства по борьбе с киберпреступностью. Была создана рабочая группа для внедрения стратегий, связанных с ГПК[910]. Ответ на вопрос о том, как возможный типовой закон взаимодействует с существующими стандартами, зависит от подхода, принятого при разработке нового типового закона. В целом есть три варианта связи:

- спорные регуляторные положения

  Если новый типовой закон определяет стандарты, которые не согласованы с существующими стандартами, это, по крайней мере, на начальном этапе может оказать негативное воздействие на необходимый процесс гармонизации.

- частичное дублирование стандартов Конвенции

  Новый типовой закон может основываться на Конвенции о киберпреступности и может исключать те положения, которые создавали трудности при подписании Конвенции или даже препятствовали ее подписанию некоторыми странами. Примером такого спора является обсуждение положений Статьи 32b Конвенции о киберпреступности. Эти положения были подвергнуто критике со стороны российской делегации на заседании Комитета по киберпреступности в 2007 году[911].

- дополнение стандартов Конвенции

  Новый типовой закон может выйти за рамки стандартов, определенных Конвенцией о киберпреступности, и, например, преследовать судебным порядком некоторые действия, связанные с киберпреступностью, и определять процессуальные инструменты, которые пока еще не описаны в Конвенции. Начиная с 2001 года выполнено несколько важных разработок. Когда Конвенция разрабатывалась ни "фишинг"[912], ни "кража идентичности"[913], ни преступления, связанные с онлайновыми играми, ни социальные сети еще не имели такого значения, как сейчас. Новый типовой закон сможет продолжить процесс гармонизации за счет включения в него будущих преступлений транснационального масштаба[914].

---

[908] For more information see http://www.itu.int/osg/csd/cybersecurity/gca/.

[909] 1. Elaboration of strategies for the development of a model cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures, 2. Elaboration of strategies for the creation of appropriate national and regional organizational structures and policies on cybercrime. 3. Development of a strategy for the establishment of globally accepted minimum security criteria and accreditation schemes for software applications and systems. 4. Development of strategies for the creation of a global framework for watch, warning and incident response to ensure cross-border coordination between new and existing initiatives.5. Development of strategies for the creation and endorsement of a generic and universal digital identity system and the necessary organizational structures to ensure the recognition of digital credentials for individuals across geographical boundaries. 6. Development of a global strategy to facilitate human and institutional capacity-building to enhance knowledge and know-how across sectors and in all the above-mentioned areas. 7. Advice on potential framework for a global multi-stakeholder strategy for international cooperation, dialogue and coordination in all the above-mentioned areas.

[910] See: http://www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

[911] Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/combating_economic_crime/6_cybercrime/t%2Dcy/FINAL%20T-CY%20_2007_%2003%20-%20e%20-%20Report%20of%20the%20meeting1.pdf.

[912] The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon phishing see *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, , available at: http://www.usdoj.gov/opa/report_on_phishing.pdf,

[913] For an overview about the different legal approaches see: *Gercke*, Internet-related Identity Theft, 2007, available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; See as well: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: http://www.privacyrights.org/ar/id_theft.htm.Regarding the economic impact see for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[914] There are two aspects that need to be taken into consideration in this context: to avoid redundancy, a new approach should focus on offences that are not intended to be covered within further amendments of the Convention on Cybercrime. The second aspect is related to the difficulties in finding a common position all countries can agree on. Based on the experiences with the negotiations of the Convention on

В этом отношении набор инструментов МСЭ для законодательства по киберпреступности[915] предназначен для предоставления странам рекомендательных материалов, которые могут помочь им в создании законодательной основы для сдерживания киберпреступности. Он подчеркивает важность для стран гармонизации их законодательных рамок в целях более эффективной борьбы против киберпреступлений и содействия международному сотрудничеству. Разработкой набора инструментов МСЭ для законодательства по киберпреступности занимается многопрофильная международная группа экспертов, и первый проект был представлен в начале 2009 года.

5.5 Взаимосвязь между различными международными и национальными подходами

Как отмечалось ранее, киберпреступность является действительно транснациональной преступностью[916]. В связи с тем, что преступники могут, в целом, выбрать в качестве цели пользователей из любой страны мира, международное сотрудничество органов охраны правопорядка является обязательным требованием для международного расследования киберпреступлений[917]. Расследования требуют наличия среды для сотрудничества и зависят от согласованности законов. Из-за общего принципа обоюдной уголовной ответственности[918], эффективное сотрудничество, в первую очередь, требует гармонизации положений материального уголовного права в целях предотвращения создания "зон безопасности" для преступников[919]. Кроме того, необходимо гармонизировать следственные инструменты, для того чтобы обеспечить все страны, вовлеченные в международное расследование, необходимыми для завершения расследования на месте следственными инструментами. Наконец, эффективное сотрудничество органов охраны правопорядка требует эффективных процедур, связанных с практическими аспектами[920]. Для любой национальной стратегии борьбы против киберпреступности важность механизмов гармонизации и необходимость участия в глобальном процессе гармонизации является, по крайней мере, тенденцией, если не необходимостью.

5.5.1 Причины популярности национальных подходов

Несмотря на широкое признание важности гармонизации, процесс внедрения международных законодательных стандартов еще далек от завершения[921]. Одной из причин того, почему национальные подходы играют важную роль в борьбе с киберпреступностью, является то, что воздействие этих преступлений не одинаково. Один из примеров – подход к борьбе со спамом[922]. Спам, связанный с электронной почтой, особенно воздействует на развивающиеся страны, и этот вопрос был проанализирован в докладе ОЭСР[923]. Из-за недостаточных и более дорогостоящих ресурсов в развивающихся странах спам оказывается гораздо более серьезной проблемой, чем в западных странах[924]. Различное влияние киберпреступности наряду с существующей законодательной структурой и традициями, являются главными причинами для значительного числа законодательных инициатив на национальном уровне, которые не являются, или только частично, посвященными внедрению международных стандартов.

Cybercrime, it is likely that negotiations of criminalisation that go beyond the standards of the Convention will proceed with difficulties.

915 Further information on the ITU Cybercrime Legislation Toolkit is available at: http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html.

916 Regarding the extent of transnational attacks in the most damaging cyber attacks see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

917 Regarding the need for international cooperation in the fight against Cybercrime see: Putnam/Elliott, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq*. available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq*. available at: http://media.hoover.org/documents/0817999825_1.pdf.

918 Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations is currently addressed in a number of international conventions and treaties. One example is Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

919 Regarding the dual criminality principle in international investigations see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf.

920 See Convention on Cybercrime, Art. 23 – Art. 35.

921 See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq.*

922 See above: Chapter 2.6.7.

923 See Spam Issue in Developing Countries. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

924 See Spam Issue in Developing Countries, Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

5.5.2 Международные решения против национальных

Во время технической глобализации может показаться немного неожиданным обсуждение того, как кто-то, желающий соединиться с интернетом, должен выбрать установленные технические стандартные протоколы[925]. Единые стандарты являются одним из основных требований для работы в сети. Однако в отличие от технических стандартов, законодательные стандарты все еще отличаются друг от друга[926]. Необходимо спросить, смогут ли национальные подходы продолжать работать с учетом международного размаха киберпреступности[927]. Этот вопрос является актуальным для всех национальных и региональных подходов, которые реализуют законодательство, не соответствующее существующим международным стандартам. Отсутствие гармонизации может серьезно затруднить международные расследования, тогда как национальные и региональные подходы, следующие за международными стандартами, позволяют избежать проблем и трудностей в ходе международных расследований[928].

Существуют две основные причины для растущего числа региональных и национальных подходов. Во-первых, это скорость разработки законов. Совет Европы не может заставить ни одно из его государств-членов, подписавших Конвенцию о киберпреступности, ее ратифицировать. По этой причине процесс гармонизации часто считается более медленным, чем национальные и региональные законодательные подходы[929]. В отличие от Совета Европы, Европейский союз имеет средства, чтобы заставить государства-члены внедрить рамочные решения и директивы. Именно по этой причине целый ряд стран Европейского Союза, которые подписали Конвенцию о киберпреступности в 2001 году, но еще не ратифицировали ее, тем не менее, приняли в 2005 году Рамочное решение ЕС по атакам на информационные системы.

Вторая причина связана с национальными и региональными различиями. Некоторые преступления преследуются судебным порядком лишь в некоторых странах региона. Примерами этого являются религиозные преступления[930]. Хотя маловероятно, что будет возможна международная гармонизация уголовного законодательства, связанного с преступлениями в отношении религиозных символов, в этом отношении национальный подход может обеспечить такое положение дел, при котором законодательные стандарты могут поддерживаться в отдельной стране.

5.5.3 Сложности национальных подходов

Национальные подходы сталкиваются с рядом проблем. Что касается традиционных преступлений, то решение одной или нескольких стран преследовать некоторые деяния судебным порядком, может оказать влияние на возможность совершения преступлений в этих странах. Однако когда речь идет о преступлениях, связанных с интернетом, способность одной страны повлиять на преступника гораздо меньше, поскольку преступник, в целом, может действовать из любого места, где имеется подключение к сети[931]. Если они действуют из стран, которые где определенные деяния судебным порядком не преследуются, то международные расследования, а также просьбы о выдаче часто будут безуспешными. Одна из основных целей международных законодательных подходов состоит в том, чтобы предотвратить создание таких зон безопасности путем продвижения и применения мировых стандартов[932]. В результате национальные подходы в целом требуют дополнительных сторонних мер, которые должны работать[933]. Наиболее популярные дополнительные меры:

- Судебное преследование пользователя, а не только поставщика незаконного содержания

---

925 Regarding the network protocols see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

926 See for example the following surveys on national Cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005 -, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework - unauthorized access to computer systems - penal legislation in 44 countries, available at: http://www.mosstingrett.no/info/legal.html.

927 Regarding the international dimension see above: Chapter 3.2.6.

928 With regard to the Convention on Cybercrime see: Explanatory Report to the Convention on Cybercrime, No. 33.

929 Regarding concerns related to the speed of the ratification process see *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 144.

930 See below: Chapter 6.1.9.

931 See above: Chapter 3.2.6 and Chapter 3.2.7.

932 The issue was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies".

933 For details see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 et seq.

Один подход заключается в судебном преследовании за использование незаконных услуг в дополнение судебному преследованию только тех, кто такие услуги предоставляет. В данном подходе применяется судебное преследование пользователей, которые находятся под данной юрисдикцией, чтобы компенсировать недостающее влияние на поставщика услуг, который действует из-за рубежа.

- Судебное преследование за услуги, используемые при совершении киберпреступления.

Второй подход заключается в регулировании и даже судебном преследовании за предоставление определенных услуг на территории под данной юрисдикцией, которые используются в преступных целях. Данное решение выходит за рамки первого подхода в том, что оно касается предприятий и организаций, предлагающих нейтральные услуги, которые используются для законной, а также незаконной деятельности. Примером такого подхода является принятие в США в 2006 году Акта о нелегальных азартных играх в интернете[934].

Тесно связано с этой мерой установление обязанностей для фильтрации определенного содержания, с которым можно ознакомиться в интернете[935]. Такой подход был обсужден в рамках известного Yahoo-решения[936], и в настоящее время обсуждается в Израиле, где поставщики услуг доступа в интернет обязаны ограничить доступ к некоторым веб-сайтам, содержащим информацию для взрослых. Попытки контролировать содержание интернета не ограничиваются только взрослым содержанием, некоторые страны используют технологию фильтрации для ограничения доступа к веб-сайтам, которые касаются политических вопросов. Инициатива OpenNet[937] сообщает о том, что цензура практикуется примерно в двух десятках стран[938].

---

934 For an overview about the law see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: http://www.gamblingandthelaw.com/columns/2006_act.htm. For more information see below: Chapter 6.1.j.

935 Regarding filter obligations/approaches see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 et. seq., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965; Regarding the discussion about filtering in different countries see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 et seq. ; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No 5.14, 18.06.2007, available at: http://www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: http://www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: http://www.ip-watch.org/weblog/index.php?p=842; Zwenne, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement , available at: http://www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf; Regarding self-regulatory approaches see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf. *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

936 See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *http://www.juriscom.net/en/uni/doc/yahoo/poullet.htm; Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

937 The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others the Harvard Law School and the University of Oxford participate in the network. For more information see: http://www.opennet.net.

938 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: http://www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

6 ПРАВОВЫЕ РЕЗУЛЬТАТЫ

В следующей главе представлен обзор вариантов правового реагирования на явление киберпреступности путем объяснения правовых подходов в случае судебного преследования определенных деяний[939]. Там, где возможно, будут приводиться международные подходы. В случаях, когда международные подходы отсутствуют, будут использоваться национальные или региональные подходы.

6.1 Материальное уголовное право

6.1.1 Незаконный доступ (хакерство)

С начала развития компьютерных сетей, их возможностей соединений компьютеров и предоставления пользователям доступа к другим компьютерным системам хакеры использовали компьютеры для преступных целей[940]. В действиях хакеров существуют существенные различия[941]. Хакерам не обязательно присутствовать на месте преступления[942]; им всего лишь требуется обойти защиту, обеспечивающую безопасность сети[943]. Во многих случаях незаконного доступа системы безопасности, защищающие местонахождение аппаратных средств сети, являются более сложными по сравнению с системами безопасности, защищающими важную информацию в сетях, даже находящихся в том же здании[944].

Незаконный доступ к компьютерным системам мешает операторам компьютеров спокойно и свободно управлять, работать и контролировать свои системы[945]. Задачей защиты является поддержание сохранности компьютерных систем[946]. Очень важно различать незаконный доступ и повторяющиеся преступления, например информационный шпионаж[947], так как правовые нормы имеют разный подход к защите. В большинстве случаев незаконный доступ, когда закон пытается обеспечить сохранность самой компьютерной системы, не является конечной целью, а скорее, первым этапом дальнейших преступлений, например, изменение или получение доступа к хранящимся данным, когда закон пытается обеспечить сохранность и конфиденциальность данных[948].

Вопрос заключается в том, должно ли действие по незаконному доступу рассматриваться как преступление вместе с последующими преступлениями[949]? Анализ различных подходов к судебному преследованию незаконного доступа к компьютеру на национальном уровне показывает, что законодательные положения иногда смешивают незаконный доступ с последующими преступлениями или стараются ограничить судебное преследование незаконного доступа только случаями тяжких преступлений[950]. В некоторых странах преступлением считается обычный доступ, а в других судебное преследование применяется только к тем

---

939 For an overview about legal approaches see also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18 et seq., available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

940 *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No5 – page 825 et sqq.

941 These range from the simple proof that technical protection measures can be circumvented, to the intention of obtaining data stored on the victimised computer. Even political motivations have been discovered. See: *Anderson*, "Hacktivism and Politically Motivated Computer Crime", 2005, available at: http://www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf;

942 Regarding the independence of place of action and the location of the victim, see above 3.2.7.

943 These can for example be passwords or fingerprint authorisation. In addition, there are several tools available that can be used to circumvent protection measures. For an overview of potential tools, see *Ealy*, "A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention", available at: http://www.212cafe.com/download/e-book/A.pdf.

944 Regarding the supportive aspects of missing technical protection measures, see *Wilson*, "Computer Attacks and Cyber Terrorism, Cybercrime & Security", IIV-3, page 5. The importance of implementing effective security measures to prevent illegal access is also highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 45.

945 *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, Page 729.

946 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 44. "*The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner*".

947 With regard to data espionage see above, Chapter 2.4.b and below, Chapter 6.1.2.

948 With regard to data interference see above, Chapter 2.4.d and below, Chapter 6.1.3.

949 *Sieber*, Informationstechnologie und Strafrechtsreform, Page 49 et seq.

950 For an overview of the various legal approaches towards criminalising illegal access to computer systems, see *Schjolberg*, "The Legal Framework - Unauthorized Access To Computer Systems - Penal Legislation In 44 Countries, 2003", available at: http://www.mosstingrett.no/info/legal.html.

преступлениям, когда система, к которой получен доступ, защищается системами безопасности, или когда злоумышленник имел преступные намерения, или когда были получены, изменены или повреждены данные[951]. Другие страны преступлением считается не сам доступ, а только последующие преступления[952]. Противники судебного преследования незаконного доступа ссылаются на ситуации, когда в процессе простого доступа не создавалась опасность или когда деяния "хакерства" приводили к обнаружению дыр и слабых мест в системах безопасности атакованных компьютерных систем[953].

Конвенция о киберпреступности

Конвенция о киберпреступности включает в себя положение по незаконному доступу с целью защиты целостности компьютерных систем путем судебного преследования незаконного доступа к системе. Отмечая противоречивые подходы на национальном уровне[954], в Конвенции предлагается возможность ограничений, которые, по крайней мере, в большинстве случаев позволят странам без существующих законопроектов сохранить более либеральные законы в отношении незаконного доступа[955].

Положение

> ***Статья 2 – Незаконный доступ***
>
> *Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву доступ, когда он является преднамеренным, к компьютерной системе в целом или любой ее части без права на это. Любая Сторона может требовать, чтобы такие деяния считались преступными, если они совершены с нарушениями мер безопасности и с намерением завладеть компьютерными данными или иным злым умыслом, или в отношении компьютерной системы, соединенной с другой компьютерной системой.*

Охватываемые действия

Термин "доступ" не определяет конкретные средства связи, а является неокончательным и допускает дальнейшие технические поправки[956]. Он будет включать в себя как все средства доступа к другой компьютерной системе, включая атаки через интернет[957], так и незаконный доступ к беспроводным сетям. Настоящее положение касается даже незаконного доступа к компьютерам, которые не объединены в какие-

---

951 Art. 2 Convention on Cybercrime enables the member states to keep those existing limitations that are mentioned in Art. 2, sentence 2 Convention on Cybercrime. Regarding the possibility to limit the criminalisation see as well: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 40.

952 An example of this is the German Criminal Code, which criminalised only the act of obtaining data (Section 202a). This provision was changed in 2007. The following text presents the old version:
Section 202a - Data Espionage
(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.
(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

953 This approach is not only found in national legislation, but was also recommended by the Council of Europe Recommendation N° (89) 9.

954 For an overview of the various legal approaches in criminalising illegal access to computer systems, see *Schjolberg*, "The Legal Framework - Unauthorized Access To Computer Systems - Penal Legislation In 44 Countries, 2003", available at: http://www.mosstingrett.no/info/legal.html.

955 Regarding the system of reservations and restrictions, see *Gercke*, "The Convention on Cybercrime", Computer Law Review International, 2006, 144.

956 *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

957 With regard to software tools that are designed and used to carry out such attacks see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 et seqq., available at: http://www.212cafe.com/download/e-book/A.pdf. With regard to Internet related social engineering techniques see the information offered by anti-phishing working group, available at: http://www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing , available at: http://www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606; The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

либо сети, например, при помощи обхода парольной защиты[958]. Такой широкий подход означает, что понятие незаконного доступа охватывает не только технические поправки в будущем, но доступ к секретным данным со стороны инсайдеров и персонала[959]. Второе положение Статьи 2 предлагает возможность ограничения судебного преследования незаконного доступа доступом через сеть[960].

Таким образом, незаконные действия и защищенные системы определяются так, что в эти определения можно будет вносить поправки. В Поясняющем Отчете содержится список аппаратных средств, компонентов, хранимых данных, директорий и данных, относящихся к трафику и содержимому, в качестве примера тех частей компьютерных систем, к которым можно поучить доступ[961].

Субъективная сторона

Так же, как для всех других преступлений, обозначенных Конвенцией о киберпреступности, Статья 2 требует, чтобы преступник совершал нарушение умышленно[962]. В Конвенции не содержится определение термина "умышленно". В Поясняющем Отчете авторы проекта указано, что термин "умышленно" должен определяться на национальном уровне[963].

Без права

В соответствии со Статьей 2 Конвенции, доступ к компьютеру может преследоваться по суду, если он осуществляется "без права"[964]. Доступ к системе, позволяющей общедоступный свободный и открытый доступ, или доступ к системе с позволения владельца или правообладателя не является доступом "без права"[965]. Дополнительно к предмету свободного доступа относится законность процедур по тестированию безопасности[966]. Администраторы сети и компании по безопасности, которые тестируют защиту компьютерных систем с целью определения возможных дыр в системах безопасности, предупреждены о возможности обвинения в незаконном доступе[967]. Несмотря на факт того, что эти профессионалы в основном работают с разрешения владельца, и поэтому действуют законно, авторы проекта Конвенции подчеркнули, что "тестирование или защита безопасности компьютерной системы, санкционированные владельцем или оператором, [...] осуществляются по праву"[968].

Факт того, что жертва преступления предоставила преступнику пароль или аналогичный код доступа, не всегда означает, что вследствие этого преступник действует по праву после получения доступа к компьютерной системе жертвы. Если преступник принудил жертву сообщить пароль или код доступа в

---

958 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

959 The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5% of the respondents reported that 80-100% of their losses were caused by insiders. Nearly 40% of all respondents reported that between 1% and 40% of the losses related to computer and network crimes were caused by insiders. For more details, see: 2007 CSI Computer Crime and Security Survey, page 12, available at: http://www.gocsi.com/.

960 Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

961 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

962 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

963 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

964 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

965 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47.

966 *Jones*, Council of Europe Convention on Cybercrime: Themes and Critiques, Page 7.

967 See for example: World Information Technology And Services Alliance (WITSA), "Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000", available at: http://www.witsa.org/papers/COEstmt.pdf; "Industry group still concerned about draft Cybercrime Convention, 2000", available at: http://www.out-law.com/page-1217.

968 Explanatory Report to the Council of Europe Convention on Cybercrime No. 47 and Explanatory Report to the Council of Europe Convention on Cybercrime No. 62" (Dealing with Article 4).

результате удачного применения методов психологического воздействия[969], необходимо подтверждение того, что разрешение, предоставленное жертвой, относится ко всем действиям, предпринятым преступником[970]. Как правило дело обстоит иначе, и потому преступник действует без права.

Ограничения и оговорки

В качестве альтернативы широкому подходу Конвенция предлагает возможность ограничения судебного преследования дополнительными элементами, перечисленными во втором предложении[971]. Процедура применения данного ограничения описана в Статье 42 Конвенции[972]. Возможные ограничения относятся к мерам безопасности[973], особым намерениям получения компьютерных данных[974], другим мошенническим намерениям, которые доказывают уголовную ответственность, или требованиям, используемым при преступлении против компьютерной системы через сеть[975]. Схожий подход можно найти в Рамочном Решении ЕС[976] касательно атак на информационные системы[977].

Типовой закон Содружества о компьютерах и компьютерных преступлениях

Схожий подход можно найти в Разделе 5 Типового закона Содружества[978] 2002 года.

> ***Раздел 5***
>
> *Лицо, намеренно, без правомерной причины или объяснения, получившее доступ ко всей или любой части компьютерной системы, совершает преступление, караемое по приговору тюремным заключением на срок, не превышающий [период], или штрафом, не превышающим [значение], или и тем и другим.*

Главным отличием от Конвенции о киберпреступности является тот факт, что Раздел 5 Типового закона Содружества, в отличие от Статьи 2 Конвенции о киберпреступности, не содержит возможности оговорок.

---

969 *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: http://www.securityfocus.com/infocus/1527.

970 This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: http://www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606; The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

971 *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

972 Article 42 – Reservations*: By a written notification addressed to the Secretary-General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.*

973 This limits the criminalisation of illegal access to those cases where the victim used technical protection measures to protect it's computer system. Access an unprotected computer system would therefore not be considered a criminal act.

974 The additional mental element/motivation enables the member states to undertake a more focused approach not implement a criminalisation of the mere hacking. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 47 and Explanatory Report to the Council of Europe Convention on Cybercrime No. 62

975 This enables the member states to avoid a criminalisation of cases where the offender had physical access to the computer system of the victim and therefore did not need to perform an Internet-based attack.

976 Framework Decision on attacks against information systems – 19. April 2002 – COM (2002) 173. For more details see above: Chapter 5.1.e.

977 *Article 2 - Illegal access to information systems:*

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases that are not minor.

2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

978 "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

Проект Стэнфордской Конвенции

Неофициальный[979] проект Стэнфордской Конвенции от 1999 года определяет незаконный доступ как одно из преступлений, которое должно преследоваться по закону в государствах, подписавших ее.

Положение

> ***Статья 3 – Преступления***
>
> *1. Преступлением согласно настоящей Конвенции считается, если любое лицо незаконно и намеренно участвует в любом из перечисленных далее действий без законно подтвержденных санкций, разрешений или согласия:*
>
> *[...]*
>
> *c) входит в киберсистему, доступ к которой очевидно и недвусмысленно запрещен;*
>
> *[...]*

Охватываемые действия

В проекте положений прослеживается ряд соответствий Статье 2 Конвенции о киберпреступности. Обе требуют преднамеренного действия, совершаемого без права/без санкции. В таком контексте требования проекта положений ("*без законно подтвержденных санкций, разрешений или согласия"*) имеют более четкое значение, чем термин "без права"[980], используемый в Конвенции по киберпреступности, и однозначно направлены на внедрение концепции самозащиты[981]. Главным отличием от Конвенции является то, что в проекте положений используется термин "киберсистема". Киберсистема определяется в параграфе 3 Статьи 1 Проекта Конвенции. Она описывает любой компьютер или компьютерную сеть, используемые для ретрансляции, передачи, координации или управления связью данных или программ. Это определение демонстрирует большое сходство с определением термина "компьютерная система", представленным в Статьи 1 a) Конвенции по киберпреступности[982]. Несмотря на то, что проект Конвенции ссылается на действия, связанные с обменом данными, и поэтому в основном сосредоточен на компьютерных системах на основе сетей, оба определения включают в себя как компьютер, находящийся в сети, так и отдельные машины[983].

---

[979] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[980] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[981] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[982] In this context "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;

[983] Stand alone computer system are covered by Art. 1, paragraph 3 of the Draft Convention because they "control programs". This does not require a network connection.

6.1.2 Информационный шпионаж

И Конвенция о киберпреступности, и Типовой закон Содружества, и Проект Стэнфордской Конвенции предлагают правовые решения только для незаконного перехвата[984]. Вызывает сомнения, применима ли Статья 3 Конвенции по киберпреступности к другим случаям, отличающимся от тех, когда преступления осуществляются путем перехвата процессов передачи данных. Как указывается ниже[985], вопрос охватывает ли незаконный доступ к информации, хранящейся на жестком диске, Конвенцией, обсуждался с большим интересом[986]. Так как необходимы процессы передачи, вероятно, что Статья 3 Конвенции о киберпреступности не охватывает видов информационного шпионажа, отличных от перехвата процессов передачи[987].

Одним из часто обсуждаемых в данном контексте вопросов является вопрос, не делает ли судебное преследование незаконного доступа излишним судебное преследование информационного шпионажа. В тех случаях, когда преступник имеет законный доступ к компьютерной системе, например, ему поручено ее отремонтировать, и потому, нарушая ограничения данного разрешения, он копирует файлы из системы, то данное деяние в целом не охватывается положениями, о судебном преследовании незаконного доступа[988].

Учитывая, что сегодня большой объем важных данных хранится в компьютерных системах, необходимо определить, работают ли существующие механизмы защиты данных или требуется создание положений уголовного права для защиты пользователя от информационного шпионажа[989]. Сегодня пользователи компьютеров могут использовать различные аппаратные устройства и программные продукты для защиты важной информации. Они могут установить брэндмауэр, системы контроля доступа или шифровать хранящуюся информацию, уменьшая тем самым риск информационного шпионажа[990]. Несмотря на то, что доступны устройства с дружественным интерфейсом, требующие от пользователя минимальных знаний, действительно эффективная защита данных в компьютерной системе часто требует знаний, имеющихся у ограниченного числа пользователей[991]. В особенности часто недостаточно защищены от информационного шпионажа данные, хранящиеся в частных компьютерных системах. Поэтому дополнительную защиту могут предоставить положения уголовного права.

Примеры

Некоторые страны решили распространить защиту, доступную при помощи технических средств, узаконив судебное преследование информационного шпионажа. Существуют два основных подхода. Некоторые страны следуют узкому подходу и преследуют по суду информационный шпионаж, только когда он относится к определенному виду секретной информации, например 18 U.S.C п. 1831, в котором определено судебное

---

984 The Explanatory Report points out, that the provision intends to criminalise violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

985 See below: Chapter 6.1.c.

986 See *Gercke*, "The Convention on Cybercrime", Multimedia und Recht 2004, page 730.

987 One key indication of the limitation of the application is the fact that the Explanatory Report compares the solution in Art. 3 to traditional violations of the privacy of communication beyond the Internet that do not cover any form of data espionage. *"The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights."* See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

988 See in this context especially a recent case from Hong Kong, People's Republic of China. See above: Chapter 2.4.2.

989 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

990 Regarding the challenges related to the use of encryption technology by offenders see above: Chapter 3.2.m; *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf.; *Zanini/Edwards*, "The Networking of Terror in the Information Age", in *Arquilla/Ronfeldt*, "Networks and Netwars: The Future of Terror, Crime, and Militancy", page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf. *Flamm*, "Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography", available at: http://www.terrorismcentral.com/Library/Teasers/Flamm.html.Regarding the underlying technology see: *Singh*; "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography", 2006; *D'Agapeyen*, "Codes and Ciphers – A History of Cryptography", 2006; "An Overview of the History of Cryptology", available at: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

991 One of the consequences related to this aspect is the fact, that the limitation of a criminalisation of illegal access to those cases, where the victim of the attack secured the target computer system with technical protection measures could limit the application of such provision as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

преследование экономического шпионажа. Это положение охватывает не только информационный шпионаж, но и другие способы получения секретной информации.

> ***§ 1831 Экономический шпионаж***
>
> *a) В целом любой, намеревающийся или знающий, что это преступление будет выгодно любому иностранному правительству, иностранному агентству или иностранному агенту, намеренно*
>
> *1) крадет, или без разрешения присваивает, берет, уносит или скрывает, или получает коммерческую тайну путем обмана, махинаций или хитрости;*
>
> *2) без разрешения копирует, дублирует, делает набросок, рисунок, фотографию, скачивает, закачивает, изменяет, уничтожает, ксерокопирует, тиражирует, доставляет, пересылает, отправляет, в том числе по почте, сообщает или переправляет коммерческую тайну;*
>
> *3) получает, покупает или завладевает коммерческой тайной, одновременно сознавая, что она украдена, или получена, или захвачена или преобразована без разрешения;*
>
> *4) пытается совершить любое преступление, описанное в любом параграфе с 1) по 3); или*
>
> *5) вступает в сговор с одним или несколькими лицами для совершения любого преступления, описанного в любом параграфе с 1) по 3),и одно или несколько таких лиц совершают любое действие для достижения цели сговора.*
>
> *Подтвергается, за исключением случаев, указанных в подразделе b), штрафу на сумму не более 500 000 долл. США или тюремному заключению на срок не более 15 лет, или и то и другое.*
>
> *b) Организации, любая организация, которая совершает любое преступление, описанное в подразделе a), подвергается штрафу на сумму не более 10 000 000 долл. США.*

В других странах принят более широкий подход и криминализируется действие по получению хранящихся в компьютере данных, даже если они не содержат экономических секретов. В качестве примера служит предыдущая редакция п. 202a Уголовного кодекса Германии[992].

> ***Раздел 202a Информационный шпионаж***
>
> *1) Любое лицо, получившее для себя или другого лица без разрешения, данные, которые ему не предназначены и которые особо защищены от несанкционированного доступа, подвергается тюремному заключению на срок, не превышающий три года, или штрафу.*
>
> *2) К данным, охватываемым подразделом 1, относятся только хранящиеся или передаваемые в электронном или магнитном виде или любой форме, не видимой невооруженным глазом.*

Это положение охватывает не только коммерческие секреты, но и хранящиеся на компьютере данные в целом[993]. На основе объектов защиты этот поход шире, чем в § 1831 USC, но применение этого положения ограничено, так как получение данных криминализируется только в случаях особой защиты от несанкционированного доступа[994]. Таким образом, в соответствии с Уголовным кодексом Германии, защита хранящихся на компьютере данных ограничивается лицами или компаниями, принявшими меры по предотвращению возможностей таких преступлений[995].

---

[992] This provision has recently been modified and now even criminalises illegal access to data. The previous version of the provision was used, because it is suitable to demonstrate the dogmatic structure in a better way.

[993] See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.

[994] A similar approach of limiting criminalisation to cases where the victim did not take preventive measures can be found in Art. 2, sentence 2, Convention on Cybercrime: *A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.* For more information see above: Chapter 6.1.1.

[995] This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement self protection measures.

Важность таких положений

Внедрение таких положений особенно важно в тех случаях, когда преступник имел разрешение для доступа к компьютерной системе, например, ему было поручено исправить проблемы с компьютером, а затем злоупотребил разрешением для незаконного получения информации, хранящейся в компьютерной системе[996]. Учитывая факт, что разрешение охватывает доступ к компьютерной системе, в целом невозможно охватить законами криминализацию незаконного доступа.

Без права

Применение положений по информационному шпионажу в целом требует, чтобы данные были получены без согласия жертвы. Успех фишинг-атак[997] очевидно демонстрирует успех афер на основе манипуляций пользователями[998]. Вследствие согласия жертвы, преступники, преуспевшие в манипуляции пользователями для обнаружения секретной информации, не могут преследоваться на основе вышеупомянутых положений.

6.1.3 Незаконный перехват

Использование ИКТ сопровождается группой рисков, относящихся к безопасности передачи информации[999]. В отличие от классических действий по почтовой пересылке внутри страны, процессы передачи данных по интернету включают в себя множество поставщиков и различные точки, где процесс передачи данных может быть перехвачен[1000]. Самым уязвимым пунктом остается пользователь, особенно пользователи частных домашних компьютеров, которые зачастую недостаточно защищены от внешних атак. Так как злоумышленники практически всегда нацеливаются на самый уязвимый объект, риск атак на частных пользователей велик, тем более, что наблюдается:

- развитие уязвимых технологий; и
- постоянно растущая ценность личной информации для злоумышленников.

Новые технологии сети, например беспроводные ЛВС, предоставляют некоторые преимущества для доступа в интернет[1001]. Создание беспроводной сети в частном доме, например, позволяет семье подключаться к интернету из любой точки в пределах определенного радиуса без кабельных соединений. Но популярность этой технологии и получающиеся удобства сопровождаются серьезными рисками для безопасности сети. Если существует незащищенная беспроводная сеть, злоумышленники могут подключиться к данной сети и использовать ее для преступных действий без необходимости получения доступа в здание. Для осуществления атаки им просто нужно

---

[996] See in this context for example a recent cases in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: http://www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadros*, Stolen photos from laptop tell a tawdry tale, The Sydney Morning Harald, 14.02.2008, available at: http://www.smh.com.au/news/web/stolen-photos-from-laptop-tell-a-tawdry-tale/2008/02/14/1202760468956.html; Pomfret, Hong Kong's Edision Chen quits after sex scandal, Reuters, 21.02.2008, available at: http://www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: http://www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

[997] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see above: Chapter 2.8.d.

[998] With regard to "phishing" see above: Chapter 2.8.d and below: Chapter 6.1.n and as well: *Jakobsson*, The Human Factor in Phishing, available at: http://www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606; The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

[999] Regarding the risks related to the use of wireless networks, see above: Chapter 3.2.c. Regarding the difficulties in Cybercrime investigations that include wireless networks, see *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime" " in Cybercrime & Security, IIA-2; Urbas/Krone, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: http://www.aic.gov.au/publications/tandi2/tandi329t.html.

[1000] Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1001] Regarding the underlying technology and the security related issues see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: http://www.infodev.org/en/Document.18.aspx. With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: "The Wireless Internet Opportunity for Developing Countries, 2003", available at: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

попасть в пределы беспроводной сети. Полевые испытания показывают, что примерно 50% частных беспроводных сетей не защищены от несанкционированного перехвата или доступа[1002]. В большинстве случаев недостаток защиты происходит из-за нехватки знаний о настройке мер безопасности[1003].

В прошлом злоумышленники в основном интересовались незаконным перехватом данных в промышленных сетях[1004]. Перехват промышленных передач позволял получать больше полезной информации, чем данные, передаваемые в частных сетях. Увеличивающееся количество краж идентичности частных персональных данных говорит о тои, что задачи злоумышленников могли поменяться[1005]. Личные данные, например, номера кредитных карт, номера социального страхования[1006], пароли и информация о банковских счетах в настоящее время имеют большую ценность для преступников[1007].

Конвенция о киберпреступности

Конвенция о киберпреступности включает в себя положения, защищающие сохранность внутренних передач при помощи судебного преследования их несанкционированного перехвата. Это положение предназначено для приравнивания защиты электронных передач к защите голосовых переговоров от незаконного перехвата и/или записи, которая в настоящее время существует в большинстве правовых систем[1008].

Положение

> ***Статья 3 – Незаконный перехват***
>
> *Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву – преднамеренно осуществленный с использованием технических средств перехват без права на это – не предназначенных для общего пользования компьютерных данных, передаваемых в компьютерную систему, из нее или внутри такой системы, включая электромагнитные излучения компьютерной системы, несущей такие компьютерные данные. Любая Сторона может требовать, чтобы такое деяние считалось преступным, если оно было совершено со злым умыслом или в отношении компьютерной системы, соединенной с другой компьютерной системой.*

Охватываемые действия

Применение Статьи 3 ограничивается перехватом передач, осуществляемым при помощи технических средств[1009]. Перехват электронных данных может определяться как любое действие по получению данных во время процесса передачи[1010].

[1002] The computer magazine ct reported in 2004 that field tests proved that more than 50% of 1000 wireless computer networks that were tested in Germany were not protected. See: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182

[1003] Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, "Information Technology Security Handbook", page 60, available at: http://www.infodev.org/en/Document.18.aspx.

[1004] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1005] Regarding Identity Theft, see above: Chapter: 2.7.3 and below: Chapter 6.1.15 and as well: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf. *Lee*, Identity Theft Complaints Double in '02, New York Times, Jan. 22, 2003; *Gercke*, Internet-related Identity Theft, 2007, available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf; For an approach to divide between four phases see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 et seq., available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[1006] In the United States the SSN was created to keep an accurate record of earnings. Contrary to its original intentions, the SSN is today widely used for identification purposes.Regarding offences related to social security numbers see: *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: http://www.privacyrights.org/ar/id_theft.htm; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350

[1007] See: *Hopkins*, "Cybercrime Convention: A Positive Beginning to a Long Road Ahead", Journal of High Technology Law, 2003, Vol. II, No. 1; Page 112.

[1008] Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

[1009] The Explanatory Report describes the technical means more in detail: "Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalisation." Explanatory Report to the

Как упоминалось выше, вопрос о том, касается ли положение незаконного доступа к информации, хранящейся на жестком диске, всесторонне обсуждается[1011]. В целом положение применимо только к перехвату передачи, а доступ к хранящейся информации не считается перехватом передачи[1012]. Факт того, что применение приложения обсуждается даже в тех случаях, когда злоумышленник имеет физический доступ к отдельной компьютерной системе, частично возникает как результат того, что Конвенция о киберпреступности не содержит положения касательно информационного шпионажа[1013], а в Поясняющем Отчете к Конвенции содержатся два немного неточных объяснения касательно применения Статьи 3:

- прежде всего, в Поясняющем Отчете указывается на то, что положение охватывает процессы связи, происходящие внутри компьютерной системы[1014]. Однако все еще остается открытым вопрос, должно ли это положение применяться только в случаях, когда жертвы отправляют данные, которые затем перехватываются злоумышленниками, или его также следует применять, когда злоумышленник лично работает за компьютером.
- руководство указывает на то, что перехват может осуществляться либо опосредовано при помощи устройств перехвата, либо "путем доступа и использования компьютерной системы"[1015]. Если злоумышленники получают доступ к компьютерной системе и используют ее для создания несанкционированных копий хранящихся данных на внешний дисковый привод, когда действие ведет к передаче данных (отправка данных с внутреннего на внешний жесткий диск), данный процесс не *перехватывается*, а скорее *инициируется* злоумышленниками. Отсутствующий элемент технического перехвата является сильным аргументом против применения положения в случаях незаконного доступа к хранящейся информации[1016].

Термин "передача" охватывает все передачи данных: по телефону, факсу, электронной почте или передаче файлов[1017]. Преступление, подпадающее под Статью 3, применимо только к внутренним передачам[1018]. Передача является "внутренней", если процесс передачи конфиденциален[1019]. Для различия внешней и внутренней передачи важно понимать не природу передаваемых данных, а природу самого процесса передачи. Даже передача свободно доступной информации может считаться преступлением, если стороны, участвующие в передаче, намерены держать в секрете содержимое передачи. Использование общественных сетей не исключает "внутренней" передачи.

Субъективная сторона

Как и для всех других преступлений, указанных в Конвенции о киберпреступности, в Статье 3 указывается, что злоумышленник должен осуществлять преступление намеренно[1020]. В Конвенции не содержится

Council of Europe Convention on Cybercrime No. 53.

[1010] Within this context, only interceptions made by technical means are covered by the provision - Article 3 does not cover acts of "social engineering".

[1011] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, Page 730.

[1012] *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1013] See above: Chapter 6.1.2

[1014] "The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example) between two computer systems belonging to the same person, two computers communicating with one another or a computer and a person (e.g. through the keyboard)." Explanatory Report to the Council of Europe Convention on Cybercrime No. 55.

[1015] Explanatory Report to the Council of Europe Convention on Cybercrime No. 53.

[1016] Covered by Article 3 is the interception of electronic emissions that are produced during the use of a computer. Regarding this issue, see Explanatory Report No. 57: *"The creation of an offence in relation to 'electromagnetic emissions' will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as 'data' according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision";* Explanatory Report to the Council of Europe Convention on Cybercrime No. 57.

[1017] Explanatory Report to the Council of Europe Convention on Cybercrime No. 51.

[1018] *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1019] Explanatory Report to the Council of Europe Convention on Cybercrime No. 54.

[1020] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

определение термина "намеренно". В Поясняющем Отчете разработчики указали, что определение термина "намеренно" должно производиться на национальном уровне[1021].

Без права

В соответствии со Статьей 3 Конвенции перехват сообщений может преследоваться, только если это происходит "без права"[1022]. Разработчики Конвенции представили набор примеров для перехвата, которые производятся по праву:

- действия по основному обучению или по санкции участников передачи[1023];
- санкционированное тестирование или действия по защите, согласованные участниками[1024];
- законный перехват на основе положений уголовного права или в интересах национальной безопасности[1025].

Другим вопросом, возникшим при обсуждении Конвенции, был вопрос, приведет ли использование cookies к уголовному наказанию на основе Статьи 3[1026]. Разработчики указали, что общепринятые коммерческие практики, например cookies, не считаются перехватом без права[1027].

Ограничения и оговорки

В Статье 3 предлагается возможность ограничения судебного преследования посредством требования дополнительных элементов, указанных во втором предложении, включая "мошеннические намерения" или отношение к компьютерной системе, связанной с другой компьютерной системой.

Типовой закон Содружества о компьютерах и компьютерных преступлениях

Схожий подход можно найти в Разделе 8 проекта законов Содружества[1028].

> ***Раздел 8***
>
> *Лицо, которое намеренно, без правомерной причины или объяснения, перехватывает техническими средствами:*
>
> *а) любую внутреннюю передачу к, от или внутри компьютерной системы; или*

[1021] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1022] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.
[1023] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.
[1024] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.
[1025] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.
[1026] Cookies are data sent by a server to a browser and the send back each time the browser is used to access the server. Cookies are used for authentication, tracking and keeping user information. Regarding the functions of cookies and the controversial legal discussion see: *Kesan/Shah*, Deconstruction Code, Yale Journal of Law & Technology, 2003-2004, Vol. 6, page 277 et seqq., available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.
[1027] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.
[1028] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

b) электромагнитные излучения от компьютерной системы, которые являются носителями компьютерных данных; совершает преступление, караемое, по приговору, тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [значение], или и тем и другим.

Проект Стэнфордской Конвенции

Неофициальный[1029] проект Стэнфордской Конвенции 1999 года не позволяет однозначно определить перехват компьютерных данных как преступление.

6.1.4 Искажение информации

Защита материальных или физических объектов от преднамеренного повреждения является классическим элементом национального уголовного законодательства. В связи с продолжающимся переводом в цифровой вид все больше важной деловой информации хранится в виде данных[1030]. Атаки или получение такой информации может привести к финансовым потерям[1031]. Кроме удаления, изменение такой информации также может иметь крупные последствия[1032]. Предыдущая версия законодательства в некоторых странах не всегда уравнивала защиту данных с защитой материальных объектов. Это позволило злоумышленникам создавать такие виды афер, которые не приводили к уголовным санкциям[1033].

Конвенция о киберпреступности

В Статье 4 Конвенции о киберпреступности содержится положение, защищающее сохранность данных от несанкционированного искажения[1034]. Целью положения является заполнение существующих пробелов в уголовном праве некоторых стран и обеспечение для компьютерных данных и компьютерных программ защиты от намеренного причинения ущерба, идентичной той, которой пользуются физические объекты[1035].

Положение

Статья 4 – Искажение информации

1) Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных без права на это.

[1029] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1030] The difficulty with offences against the integrity of data is that identification of these violations is often difficult to prove. Therefore, the Expert Group, which drafted the Convention on Cybercrime, identified the possibility of prosecuting violations regarding data interference by means of criminal law as a necessary strategic element in the fight against cybercrime. Explanatory Report to the Council of Europe Convention on Cybercrime No. 60.

[1031] The 2007 Computer Economics Malware Report focuses on single of computer crime and analyses the impact of malware on the worldwide economy by summing up the estimated costs caused by attacks. It identified peaks in 2000 (USD 17.1 billion) and 2004 (USD 17.5 billion). For more information, see: 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code. A summary of the report is available at: http://www.computereconomics.com/article.cfm?id=1225.

[1032] A number of computer fraud scams are including the manipulation of data – e.g. the manipulation of bank account files, transfer records or data on smart cards. Regarding computer related fraud scams see above: Chapter 2.7.1 and below: Chapter: 6.1.16.

[1033] Regarding the problems related to those gaps see for example the LOVEBUG case where a designer of a computer worm could not be prosecuted due to missing criminal law provisions related to data interference. See above: Chapter 2.4.d and: CNN, "Love Bug virus raises spectre of cyberterrorism", 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, "A Critical Look at the Regulation of Cybercrime", http://www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1034] A similar approach to Art. 4 Convention on Cybercrime is found in the EU Framework Decision on Attacks against Information Systems: Article 4 - Illegal data interference: "Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor".

[1035] Explanatory Report to the Council of Europe Convention on Cybercrime No. 60.

2) Любая Сторона может оставить за собой право квалифицировать, что предусмотренные пунктом 1 деяния влекут за собой серьезный ущерб.

Охватываемые деяния

- термины "повреждения" и "порча" означают любое деяние, связанное с отрицательным изменением целостности информационного содержимого данных и программ[1036];
- "удаление" охватывает деяния, при которых информация удаляется с носителей, и считаются сравнимыми с разрушением материального объекта. При создании этого определения составители Конвенции не проводили различий между различными способами, которыми можно удалить данные[1037]. Перенос файла в виртуальную корзину не удаляет файл с жесткого диска[1038]. Даже "очистка" корзины не всегда удаляет файл[1039]. Поэтому неясно, может ли возможность восстановления удаленного файла упразднить применение положения[1040];
- "скрытие" компьютерных данных обозначает действие, которое отрицательным образом влияет на доступность данных лицу, имеющему доступ к носителям, на которых хранятся данные[1041]. Применение положения особо обсуждается по отношению к атакам[1042] Отказ в обслуживании[1043]. Во время атак данные, имеющиеся на атакованном компьютере, больше не доступны ни потенциальному пользователю, ни владельцу компьютерной системы[1044];
- термин "изменение" охватывает модификацию существующих данных, не обязательно снижающее удобство использования этих данных[1045]. Это деяние особенно относится к установке на компьютер жертвы вредоносных программ, например, шпионского ПО, вирусов или бесплатного ПО с размещенной в нем рекламой[1046].

[1036] As pointed out in the Explanatory Report the two terms are overlapping. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1037] Regarding the more conventional ways to delete files by Using Windows XP see the Information provided by Microsoft, available at: http://www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

[1038] Regarding the consequences for forensic investigations see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 et. seq. , available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1039] See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: http://www.cert.org/archive/pdf/05hb003.pdf.

[1040] The fact, that the Explanatory Report mentions that the files are unrecognisable after the process does not give any further indication with regard to the interpretation of the term. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1041] Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1042] A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, "Analysis of a Denial of Service Attack on TCP"; *Houle/Weaver*, "Trends in Denial of Service Attack Technology", 2001, available at: http://www.cert.org/archive/pdf/DoS_trends.pdf.In 2000 a number of well known US e-commerce businesses were targeted by denial of service attacks. A full list of the attacks business is provided by *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", page 4, available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.For more information see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, "Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security", Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[1043] With regard to the criminalisation of "Denial-of-Service" attacks see as well below: Chapter 6.1.5.

[1044] In addition criminalisation of "Denial of Service" attacks is provided by Art. 5 Convention on Cybercrime. See below: Chapter 6.1.5.

[1045] Apart from the input of malicious codes (e.g. Viruses and Trojan Horses), it is likely that the provision could cover unauthorised corrections of faulty information as well.

[1046] *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.
Regarding the different recognised functions of malicious software see above: Chapter 2.4.d. Regarding the economic impact of malicious software attacks see above: Chapter 2.9.1.

Субъективная сторона

Так же, как и для всех других преступлений, определенных в Конвенции о киберпреступности, Статья 4 требует, чтобы злоумышление совершал преступление умышленно[1047]. В Конвенции не содержится определение термина "умышленно". В Поясняющем Отчете составители указали, что термин "умышленно" должен определяться на национальном уровне[1048].

Без права

Так же, как и для положений, обсуждавшихся выше, эти деяния должны совершаться "без права"[1049]. Право изменять данные обсуждалось, особенно в контексте "ретрансляторов"[1050]. Ретрансляторы используются для изменения определенных данных с целью облегчения анонимной связи[1051]. В Поясняющем Отчете упоминается, что, в принципе, эти деяния учитывают законную защиту конфиденциальности и потому предпринимаются с разрешения[1052].

Ограничения и оговорки

В Статье 4 предлагается возможность ограничения судебного преследования случаями, когда причиняется серьезный ущерб, схожий подход принят в Рамочном решении ЕС по атакам на информационные системы[1053], которое позволяет государствам-членам ограничивать применение положений материального уголовного права "случаями, которые не являются незначительными"[1054].

Типовой закон Содружества о компьютерах и компьютерных преступлениях

Подход, схожий со Статьей 4 Конвенции о киберпреступности, можно найти в Разделе 8 Типового закона Содружества[1055] 2002 года.

[1047] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1048] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1049] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.
[1050] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62: "The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g., encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right." Regarding the liability of Remailer see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.
[1051] For further information, see *du Pont*, "The Time Has Come For Limited Liability For Operators Of True Anonymity Remailers In Cyberspace: An Examination Of The Possibilities And Perils", Journal Of Technology Law & Policy, Vol. 6, Issue 2, Page 176 et seq., available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.
[1052] With regard to the possible difficulties to identify offenders that made use of anonymous or encrypted information, the Convention leaves the criminalisation of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.
[1053] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.
[1054] For further information, see: *Gercke*, "The EU Framework Decision on Attacks against Information Systems", Computer und Recht 2005, page 468 et seq.
[1055] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

Раздел 6

1) Лицо, которое умышленно или по грубой неосторожности, без правомерной причины или объяснения, совершило следующие действия:

a) уничтожило или изменило данные; или

b) предоставило бессмысленные, бесполезные или недействительные данные; или

c) препятствовало, прерывало или мешало законному использованию данных; или

d) препятствовало, прерывало или мешало любому лицу законному использованию данных; или

e) препятствовало доступу к данным любому лицу, имеющему на это право;

совершает преступление, караемое, по приговору, тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [значение], или и тем и другим.

2) Подраздел 1) применяется вне зависимости от того, имеют ли действия лица временный или постоянный эффект.

Проект Стэнфордской Конвенции

В неофициальном[1056] проекте Стэнфордской Конвенции 1999 года содержится два положения, которые признают преступлением действия, связанные с помехами в компьютерных данных.

Положение

Статья 3

1 Преступлением с точки зрения Конвенции считается, когда любое лицо незаконно и умышленно участвует в любом из следующих действий без законно доказанной санкции, или согласия:

a) создает, хранит, изменяет, удаляет, передает, переадресовывает, указывает неверный адрес, воздействует или создает помехи данным или программам в киберсистеме, имея цель или зная, что такие действия вызовут отказ надлежащей работы указанной киберсистемы или другой киберсистемы, или действия по созданию функций или действий, не предусмотренных ее владельцем и рассматриваемых в данной Конвенции как незаконные;

b) создает, хранит, изменяет, удаляет, передает отклоняет, указывает неверный адрес, воздействует или создает помехи в киберсистеме с целью последующего предоставления ложной информации для причинения существенного ущерба людям или собственности;

Охватываемые действия

Основным различием между Конвенцией о киберпреступности и проектом законов Содружества является то, что проект Конвенции признает преступлением искажение данных, только когда это мешает работе компьютерной системы (Статья 3, параграф 1a), или когда деяние совершается с целью предоставления ложной информации для причинения ущерба людям или собственности (Статья 3, параграф 1b). Поэтому проект закона не считает преступлением удаление обычного текстового документа с устройства хранения данных, так как не влияет не на работу компьютера и не дает ложной информации. И Конвенция о киберпреступности, и типовой закон Содружества следуют более широкому подходу, защищая сохранность компьютерных данных без необходимых требований наличия дальнейших воздействий.

[1056] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

6.1.5 Искажения системы

Люди или компании, предлагающие услуги на основе ИКТ, зависят от работы их компьютерных систем[1057]. Отсутствие доступных веб-страниц, ставших жертвами атак Отказа в обслуживании (DOS[1058]), показывает, насколько серьезна угроза атак[1059]. Такие атаки могут вызвать серьезные финансовые потери и затронуть даже мощные системы[1060]. Компании не являются единственными целями. Эксперты по всему миру в настоящее время обсуждают возможные сценарии "кибертерроризма", принимающие во внимание важные инфраструктуры, например, энергоснабжение и услуги электросвязи[1061].

Конвенция о киберпреступности

Для защиты доступа операторов и пользователей к ИКТ в Статью 5 Конвенции о киберпреступности было включено положение, считающее преступлением умышленную задержку правомерного использования компьютерных систем[1062].

Положение

> ***Статья 5 – Искажения системы***
>
> *Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное создание, без права на это, серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.*

[1057] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1058] A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see above: Chapter 2.4.e and US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, "Analysis of a Denial of Service Attack on TCP"; *Houle/Weaver*, "Trends in Denial of Service Attack Technology", 2001, available at: http://www.cert.org/archive/pdf/DoS_trends.pdf.

[1059] For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, "Inferring Internet Denial-of-Service Activities", page 1, available at: http://www.caida.org/publications/papers/2001/BackScatter/usenixsecurity01.pdf; CNN News, One year after DoS attacks, vulnerabilities remain, at http://edition.cnn.com/2001/TECH/internet/02/08/ddos.anniversary.idg/index.html. *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", page 4, available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.For more information see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, "Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security", Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[1060] Regarding the possible financial consequences of lack of availability of Internet services due to attack, see: *Campbell/Gordon/Loeb/Zhou*, "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market", Journal of Computer Security, Vol. 11, page 431-448.

[1061] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.; Related to Cyberterrorism see above Chapter 2.8.a and *Lewis*, "The Internet and Terrorism", available at: http://www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, "Cyber-terrorism and Cybersecurity"; http://www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, "Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy", in *Arquilla/Ronfeldt*, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 et seqq., available at: http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, "Cyberterrorism, Are We Under Siege?", American Behavioral Scientist, Vol. 45 page 1033 et seqq; United States Department of State, "Pattern of Global Terrorism, 2000", in: Prados, America Confronts Terrorism, 2002, 111 et seqq.; *Lake*, 6 Nightmares, 2000, page 33 et seqq; *Gordon*, "Cyberterrorism", available at: http://www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, "Information Technology for Counterterrorism: Immediate Actions and Future Possibilities", 2003, page 11 et seqq. OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: http://www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf. *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, Page 221 – 249.

[1062] The protected legal interest is the interest of operators as well as users of computer or communication systems being able to have them function properly. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 65.

Охватываемые действия

Применение положений требует того, чтобы создавались помехи работе компьютерной системы[1063].

- "Создание помех" означает любое действие, мешающее надлежащей работе компьютерной системы[1064]. Применение положения ограничивается случаями, когда создание помех осуществляется умышленно.

Список действий, в результате которых на работу компьютерной системы совершалось отрицательное воздействие, является окончательным[1065].

- Термин "процесс ввода" не определяется ни в самой Конвенции, ни ее составителями. Учитывая, что передача упоминается в Статье 5 как дополнительное действие, термин "процесс ввода" может определяться как любое действие, связанное с использованием физических интерфейсов ввода для передачи информации в компьютерную систему, тогда как термин "передача" охватывает действие, связанное с удаленным вводом данных[1066].
- Термины "повреждение" и "порча" взаимно пересекаются и определяются составителями Конвенции в Пояснительном Отчете с учетом Статьи 4 как негативное изменение сохранности информационного содержимого данных и программ[1067].
- Термин "удаление" также был определен составителями Конвенции и Пояснительного Отчета с учетом Статьи 4 и охватывает действия, когда информация удалена с носителей хранения[1068].
- Термин "изменение" охватывает модификацию существующих данных, не обязательно снижающее удобство эксплуатации этих данных[1069].
- "Скрытие" компьютерных данных обозначает действие, которое отрицательным образом влияет на доступность данных лицу, имеющего доступ к носителям, на которых хранятся данные[1070].

Кроме того, применение данного положения ограничено случаями, когда создаваемые помехи являются "серьезными". Определение критериев, которые должны соблюдаться, для того чтобы создание помех считалось серьезным, остается на ответственности сторон[1071]. Возможные ограничения в рамках национального права может включать в себя как минимальный уровень ущерба, так и ограничения в признании преступлением только атаки на важные компьютерные системы[1072].

[1063] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1064] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1065] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1066] Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection..

[1067] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61. Regarding the fact, that the definition does not distinguish between the different ways how information can be deleted see above: Chapter 6.1.d. Regarding the impact of the different ways to delete data on computer forensics see: Casey, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 et. seq. , available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1068] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1069] Apart from the input of malicious codes (e.g. Viruses and Trojan Horses), it is therefore likely that the provision could cover unauthorised corrections of faulty information as well. .

[1070] Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1071] The Explanatory Report gives examples for implementation of restrictive criteria for serious hindering: “Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered 'serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as 'serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g., by means of programs that generate "denial of service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system)” – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 67.

[1072] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf; Although the

Применение положений относительно спама

Проводились дебаты по поводу того, следует ли рассматривать проблему спама по электронной почте[1073] в рамках Статьи 5, так как спам может перегрузить компьютерные системы[1074]. Составители однозначно высказались, что спам не обязательно ведет к "серьезным" помехам и что "действие должно считаться преступлением, только когда связь умышленно и серьезно повреждена"[1075]. Составители также указали, что стороны могут иметь разный подход к созданию помех в рамках своего национального права[1076], например, определяя, что деяния по созданию помех являются административным правонарушением или подлежат санкциям[1077].

Субъективная сторона

Так же, как и для всех других преступлений, обозначенных Конвенцией о киберпреступности, Статья 5 требует, чтобы злоумышленник совершал преступление умышленно[1078]. Это включает в себя как намерение выполнить одно из перечисленных действий, так и намерение серьезно помешать работе компьютерной системы.

В Конвенции не содержится определение термина "умышленно". В Поясняющем Отчете составители указали, что термин "умышленно" должен определяться на национальном уровне[1079].

Без права

Действие должно выполняться "без права"[1080]. Как упоминалось выше, сетевые администраторы и компании по обеспечению безопасности, проверяющие защиту компьютерных систем, боялись, что их смогут привлечь к ответственности за выполнение своей работы[1081]. Эти профессионалы работают с разрешения владельца и потому действуют в рамках закона. Кроме того, составители Конвенции однозначно высказались, что проверка безопасности компьютерной системы с разрешения владельца не является действием "без права"[1082].

---

connotation of “serious” does limit the applicability, it is likely that even serious delays of operations resulting from attacks against a computer system can be covered by the provision.

[1073] 'spam” describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam legislation worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: Chapter 2.5.g.

[1074] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[1075] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1076] Regarding legal approaches in the fight against spam see below: Chapter 6.1.l.

[1077] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1078] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1079] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1080] The element “without right” is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *“A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression ‘without right’ derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party’s government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised”*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1081] See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: http://www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: http://www.out-law.com/page-1217.

[1082] Explanatory Report to the Council of Europe Convention on Cybercrime No. 68: “The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorised by its owner or operator, or the reconfiguration of a computer’s operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalised by this article, even if it causes serious hindering.”

Ограничения и оговорки

В отличие от Статей 2–4, в Статье 5 не содержится однозначной возможности ограничения применения положения в национальном законодательстве. Тем не менее, ответственность сторон по определению тяжести преступления позволяет им ограничивать его применение. Похожий подход имеется и в Рамочном соглашении Европейского Союза[1083] по атакам на информационные системы[1084].

Типовой закон Содружества о компьютерах и компьютерных преступлениях

Подход, схожий со Статьей 5 Конвенции о киберпреступности, можно найти в Разделе 7 типового закона Содружества[1085] 2002 года.

> ***Раздел 7***
>
> *1) Лицо, которое умышленно или по грубой неосторожности, без правомерной причины или объяснения:*
>
> *a) создает помехи или вмешивается в работу компьютерной системы; или*
>
> *b) создает помехи или вмешивается в работу лица, правомочно использующего или работающего с компьютерной системой.*
>
> *совершает преступление, караемое по приговору тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [размер], или и тем и другим.*
>
> *В подразделе 1) "создавать помехи" по отношению к компьютерной системе включает в себя, но не ограничено:*
>
> *a) отключение электропитания компьютерной системы; и*
>
> *b) создание электромагнитных помех компьютерной системе; и*
>
> *c) повреждение компьютерной системы любыми способами; и*
>
> *d) ввод, удаление или изменение компьютерных данных.*

Главным отличием от Конвенции является то, что на основе Раздела 7 типового закона Содружества, преступлением признаются даже действия, совершенные по неосторожности. С таким подходом типовой закон идет даже дальше требований Конвенции о киберпреступности. Еще одним отличием является то, что определение "создания помех" в Разделе 7 типового закона Содружества содержится больше действий по сравнению со Статьей 5 Конвенции о киберпреступности.

Проект Стэнфордской Конвенции

В неофициальном[1086] проекте Стэнфордской Конвенции 1999 года содержится положение, которое признает преступлением действия, связанные с помехами компьютерным системам.

[1083] Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

[1084] Article 3 - Illegal system interference: "*Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor*".

[1085] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1086] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

Положение

> ***Статья 3***
>
> *1 Преступлением с точки зрения Конвенции считается, когда любое лицо незаконно и умышленно участвует в любом из следующих действий без законно доказанной санкции, разрешения или согласия:*
>
> *а) создает, хранит, изменяет, удаляет, передает, переадресовывает, указывает неверный адрес, воздействует или создает помехи данным или программам в киберсистеме, имея целью или зная, что такие действия приведут к отказу указанной киберсистемы или другой киберсистемы, или к созданию функций или действий, не предусмотренных ее владельцем и рассматриваемых как незаконные в рамках данной Конвенции;*

Охватываемые действия

Главным различием между Конвенцией по киберпреступности и типовым законом Содружества является то, что проект Конвенции охватывает любые действия с компьютерными системами, тогда как и Конвенция по киберпреступности, и типовой закон Содружества ограничивают судебное преследование деяниями по созданию помех работе компьютерных систем.

6.1.6 Материалы эротического или порнографического содержания

Судебное преследование и тяжесть преступления, заключающегося в нелегальном содержимом и содержимом с выраженным сексуальным содержанием в разных странах различны[1087]. Стороны, которые участвовали в обсуждении Конвенции по киберпреступности, сосредоточились на гармонизации законов, относящихся к детской порнографии, и исключили более широкое судебное преследование материалов эротического и порнографического содержания. Некоторые страны уделили внимание этой проблеме, включив положения, признающие преступлением обмен материалами порнографического содержания через компьютерные системы. Однако недостаток стандартных определений создает трудности для органов охраны правопорядка в расследовании таких преступлений, когда преступник действует в стране, где обмен материалами сексуального содержания преступлением не считается[1088].

Примеры

Примером судебного преследования обмена материалами порнографического содержания служит Раздел 184 Уголовного Кодекса Германии:

> ***Раздел 184 Распространение материалов порнографического содержания***
>
> *1) Каждый, кто совершает с материалами порнографического содержания (Раздел 11 подраздел 3)) следующие действия:*
>
> *1 предлагает, предоставляет или делает их доступными для лиц моложе восемнадцати лет;*
>
> *2 демонстрирует, размещает, представляет или любым другим способом делает их доступными в местах, доступных лицам моложе восемнадцати лет или там, где они могут их увидеть;*
>
> *3 предлагает или предоставляет им в розничной сети вне соответствующих помещений, в киосках или других торговых площадях, куда покупатели обычно не имеют доступа, посредством заказов по почте, или библиотек с коммерческим абонементом, или кружков чтения;*
>
> *3а предлагает или предоставляет их другим для использования на условиях коммерческого найма или равнозначного коммерческого оборудования, исключая магазины, не доступные лицам моложен восемнадцати лет и там, где они могут их увидеть;*

[1087] For an overview on hate speech legislation, see for example: For an overview on hate speech legislation see the data base provided at: http://www.legislationline.org. For an overview on other Cybercrime related legislation see the database provided at: http://www.cybercrimelaw.net.

[1088] Regarding the challenges of international investigation see above: Chapter 3.2.f and *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf;

4 выполняет их пересылку из-за границы на условиях торговли почтой;

5 открыто предлагает, рекламирует или рекомендует в местах, доступных лицам моложе восемнадцати лет, или там, где они могут это видеть, или посредством распространения материалов без совершения коммерческих операций через обычные торговые точки;

6 позволяет другим получать их без их просьбы;

7 демонстрирует их в общественных кинотеатрах за плату, позволяющую получать доход полностью или в значительном виде;

8 производит, получает, поставляет, хранит или импортирует их целью использования или копирования, с числом копий от 1 до 7, или чтобы предоставить такую возможность другим; или

9 экспортирует их с целью распространения или копирования за рубежом, где нарушает применяемые там уголовные нормы, или чтобы предоставлять их в свободном доступе, или чтобы сделать это возможным, должен караться тюремным заключением на срок не более года или штрафом.

Это положение основано на понятии того, что такая торговля и другой обмен материалами порнографического содержания не должны считаться преступлением, если в них не вовлечены несовершеннолетние[1089]. На такой основе закон направлен на защиту нормального развития подростков[1090]. Вопрос, имеет ли доступ к порнографии отрицательное воздействие на развитие подростков, активно обсуждается[1091]. Обмен материалами порнографического содержания между совершеннолетними лицами Разделом 184 преступлением не считается. Термин "материал" охватывает не только традиционные носители, но также и цифровое хранение[1092]. Точно так же, делать "их доступными" применимо не только к действиям вне интернета, но включает в себя случаи, когда преступник делает материалы порнографического содержания доступными на веб-сайтах[1093].

Примером подхода, идущего дальше и признающего преступлением любые материалы сексуального содержания, служит Раздел 4.C.1 проекта закона Филиппин от 2007 года № 3777 [1094].

Раздел 4.C *Преступления, относящиеся к киберсексу, без ущерба уголовному преследованию в рамках Республиканского Акта № 9208 и Республиканского Акта № 7610, каждый, любым способом рекламирующий, предлагающий или содействующий совершению акта киберсекса при помощи информационной технологии и технологии связи, например, компьютеров, компьютерных сетей, телевидения, спутников, мобильных телефонов,, но не только, […]*

Раздел 3i *Киберсекс или виртуальный секс относится к любому виду сексуальной активности или возбуждения при помощи компьютеров или сетей связи.*

Данное положение следует очень широкому подходу, так как признает преступлением любой вид сексуальной демонстрации или облегчение сексуальной активности, выполняемое при помощи интернета. В виду принципа двойной преступности[1095], международные расследования с учетом таких широких подходов испытывают трудности[1096].

[1089] For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.

[1090] *Hoernle* in Muenchener Kommentar STGB, Sec. 184, No. 5.

[1091] Regarding the influence of pornography on minors see: *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact, and Prevention, Youth & Society, Vol. 34, Marco 2003, page 330 et seq., available at: http://www.unh.edu/ccrc/pdf/Exposure_risk.pdf; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002, available at: http://findarticles.com/p/articles/mi_m2372/is_1_39/ai_87080439.

[1092] See Section 11 Subparagraph 3 Penal Code: "Audio and visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection".

[1093] *Hoernle* in Muenchener Kommentar STGB, Sec. 184, No. 28.

[1094] The draft law was not in power by the time this publication was finalised.

[1095] Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on

6.1.7 Детская порнография

Интернет становится главным инструментом торговли и обмена материалами, содержащими детскую порнографию[1097]. Главными причинами такого развития являются скорость и эффективность интернета для пересылки файлов, низкая стоимость создания и распространения и осознанная анонимность[1098]. Миллионы пользователей по всему миру могут увидеть и загрузить изображения, размещенные на веб-страницах[1099]. Одной из самых важных причин "успеха" веб-страниц, предлагающих порнографию, или даже детскую порнографию, является то, что пользователи интернета чувствуют себя более защищенными от наблюдения, сидя у себя дома и загружая материалы из интернета. Если пользователи не используют способы анонимной связи, ощущение отсутствия контроля ошибочно[1100]. Большинство пользователей интернет просто не имеют представления о том, что во время их блуждания по сети они оставляют следы[1101].

Конвенция о киберпреступности Совета Европы

Чтобы усилить и гармонизировать защиту детей от эксплуатации в сексуальных целях[1102], в Конвенцию включена статья, касающаяся детской порнографии.

Положение

> ***Статья 9 – Преступления, относящиеся к детской порнографии***
>
> *1) Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовных преступлений согласно ее внутригосударственному праву, в случае совершения преднамеренно и без права на это, следующих деяний:*
>
> *a) производство детской порнографической продукции с целью распространения через компьютерную систему;*
>
> *b) предложение или предоставление в пользование детской порнографии через компьютерную систему;*
>
> *c) распространение или передача детской порнографии через компьютерную систему;*
>
> *d) приобретение детской порнографии через компьютерную систему для себя или для другого лица;*
>
> *e) обладание детской порнографией, находящейся в компьютерной системе или на носителях компьютерных данных.*
>
> *2) Для целей пункта 1 настоящей статьи в понятие "детской порнографии" включаются материалы порнографического содержания, изображающие:*
>
> *a) участие несовершеннолетнего лица в откровенных сексуальных действиях;*
>
> *b) участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях;*
>
> *c) реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.*

Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1096] Regarding the challenges of international investigation see above: Chapter 3.2.f and See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1097] *Krone*, "A Typology of Online Child Pornography Offending", Trends & Issues in Crime and Criminal Justice, No. 279; *Cox*, Litigating Child Pornography and Obscenity Cases, Journal of Technology Law and Policy, Vol. 4, Issue 2, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue2/cox.html#enIIB.

[1098] Regarding the methods of distribution, see: *Wortley/Smallbone*, "Child Pornography on the Internet", page 10 et seq., available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication see above: Chapter 3.2.m.

[1099] It was reported that some websites containing child pornography experienced up to a million hits per day. For more information, see: *Jenkins*, "Beyond Tolerance: Child Pornography on the Internet", 2001, New York University Press. *Wortley/Smallbone*, "Child Pornography on the Internet", page 12, available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1100] Regarding the challenges related to investigations involving anonymous communication technology see above: Chapter 3.2.l.

[1101] Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

[1102] Explanatory Report to the Council of Europe Convention on Cybercrime No. 91.

3) Для целей вышеприведенного пункта 2 термин "несовершеннолетние" означает любое лицо, не достигшее 18-летнего возраста. Однако любая Сторона может устанавливать и более низкие возрастные пределы, но не ниже 16 лет.

4) Каждая Сторона может оставить за собой право не применять, полностью или частично, положения параграфа 1, подпунктов d и e, а также 2, подпунктов b и c.

Большинство стран уже признали преступлением как жестокое обращение с детьми, так и традиционные методы распространения детской порнографии[1103]. Таким образом, Конвенция не ограничивается закрытием пробелов в национальном уголовном законодательстве[1104], она также стремится гармонизировать отличающиеся постановления[1105]. В Статью 9 включены три спорных элемента:

- возраст вовлеченного лица;
- судебное преследование обладания детской порнографией; и
- создание или монтаж фиктивных изображений[1106].

Ограничение по возрасту для несовершеннолетних

Одним из самых главных отличий между национальными законодательствами является возраст вовлеченного лица. Некоторые государства определяют термин "несовершеннолетний" по отношению к детской порнографии в своих национальных законах в соответствии с определением "ребенка" в Статье 1 Конвенции ООН по Правам ребенка[1107], как все лица моложе 18 лет. Другие страны считают несовершеннолетними лиц моложе 14 лет[1108]. Схожий подход наблюдается в Рамочном соглашении ЕС 2003 года по борьбе с сексуальной эксплуатацией детей и детской порнографией[1109] и в Конвенции Совет Европы 2007 года по защите детей от сексуальной эксплуатации и сексуальному насилию[1110]. Подчеркивая важность единообразного международного стандарта, относящегося к возрасту, Конвенция определяет термин в соответствии с Конвенцией ООН[1111]. Однако, признавая значительные различия в существующих национальных законодательствах, Конвенция позволяет сторонам устанавливать разный предел возраста, но не ниже 16 лет.

Судебное преследование обладания детской порнографией

В национальных правовых системах также существуют различия в судебном преследовании обладания детской порнографией[1112]. Потребность в таком материале может привести к его производству на

[1103] *Akdeniz* in *Edwards / Waelde*, "Law and the Internet: Regulating Cyberspace"; *Williams* in *Miller*, "Encyclopaedia of Criminology", Page 7. Regarding the extend of criminalisation, see: "Child Pornography: Model Legislation & Global Review", 2006, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalisation of child pornography and Freedom of Speech in the United States see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: http://www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf. *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalisation of child pornography.

[1104] Regarding differences in legislation, see: *Wortley/Smallbone*, "Child Pornography on the Internet", page 26, available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1105] Explanatory Report to the Council of Europe Convention on Cybercrime No. 91.

[1106] For an overview of the discussion, see: *Gercke*, "The Cybercrime Convention", Multimedia und Recht 2004, page 733.

[1107] Convention on the Rights of the Child, Adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with Article 49.
Article 1. For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

[1108] One example is the current German Penal Code. The term "child" is defined by law in Section 176 to which the provision related to child pornography refers: Section 176: "Whoever commits sexual acts on a person under fourteen years of age (a child) ...".

[1109] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[1110] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No: 201, available at: http:// http://conventions.coe.int.

[1111] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

[1112] Regarding the criminalisation of the possession of child pornography in Australia, see: *Krone*, "Does thinking make it so? Defining online child pornography possession offences" in "Trends & Issues in Crime and Criminal Justice", No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalisation of child pornography.

постоянной основе[1113]. Обладание такими материалами может содействовать сексуальному насилию над детьми, поэтому разработчики считают, что единственным эффективным методом сокращения производства детской порнографии является признание обладания ей незаконным[1114]. Однако в параграфе 4 Конвенции сторонам позволяется исключать судебное преследование простого обладания, ограничив ответственность только производством, предложением и распространением детской порнографии[1115].

Создание или монтаж фиктивных изображений

Хотя разработчики пытались улучшить защиту детей от сексуальной эксплуатации, правовые интересы, охватываемые параграфом 2 шире. Параграф 2 a) прямо направлен на защиту детей от жестокого обращения. Параграфы 2 b) и 2 c) охватывают изображения, сделанные без ущемления прав ребенка, например, изображения созданные при помощи программ 3D-моделирования[1116]. Причиной судебного преследования фиктивной детской порнографии является то, что эти изображения могут, не обязательно нанося вред реальному ребенку, использоваться для склонения детей к участию в таких действиях[1117].

Субъективная сторона

Так же как и для всех других преступлений, обозначенных Конвенцией о киберпреступности, Статья 9 требует, чтобы злоумышленник совершал преступление умышленно[1118]. В Пояснительном Отчете разработчики четко указали, что взаимодействие с детской порнографией без какого-либо умысла не рассматривается Конвенцией как преступление. Отсутствующий умысел может быть особенно важен, когда злоумышленник случайно открыл веб-страницу с изображениями, содержащими детскую порнографию, и, несмотря на то, что он сразу же закрыл веб-страницу, некоторые изображения были сохранены во временных папках или кэш-файлах.

Без права

Действия, относящиеся к детской порнографии, могут преследоваться в рамках Статьи 9 Конвенции, только когда они происходят "без права"[1119]. Разработчики Конвенции не дали более подробного определения, в каких случаях пользователь действует без санкции. В целом действие не выполняется "без права", только когда сотрудники органов охраны правопорядка действуют в рамках расследования.

Конвенция Совета Европы по защите детей

Другой подход к судебному преследованию действий, связанных с детской порнографией, приведен в Статье 20 Конвенции Совета Европы по защите детей от сексуальной эксплуатации и сексуального насилия[1120].

[1113] See: "Child Pornography: Model Legislation & Global Review", 2006, page 2, available at: http://www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[1114] Explanatory Report to the Council of Europe Convention on Cybercrime No. 98.

[1115] *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1116] Based on the National Juvenile Online Victimisation Study, only 3% of the arrested internet-related child pornography possessors had morphed pictures. *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 9, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

[1117] Explanatory Report to the Council of Europe Convention on Cybercrime No. 102.

[1118] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1119] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1120] Council of Europe - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

Положение

Статья 20 – Преступления, связанные с детской порнографией

1) Каждая сторона принимает необходимые законодательные или другие меры, которые могут быть для того, чтобы удостовериться, что следующее умышленное деяние, предпринимаемое без права, преследуется судебном порядком:

a) производство детской порнографии;

b) предложение или создание доступности детской порнографии;

c) распространение или передача детской порнографии;

d) производство детской порнографии для себя или другого лица;

e) обладание детской порнографии;

f) сознательное получение доступа, при помощи информационных технологий и технологий связи, к детской порнографии.

2) Для целей данной статьи термин "детская порнография" означает любой материал, изображающий ребенка, участвующего в реальном или фиктивном действии с откровенным сексуальным содержимым или любое изображение детских половых органов в основном с сексуальными целями.

3) Каждая сторона может оставить за собой право не применять, полностью или частично, параграфы 1 a) и e) к производству и обладанию материалами порнографического содержания:

– *состоящих полностью из фиктивных изображений или реалистичных изображений несуществующего ребенка;*

– *вовлечение детей, достигших возраста, указанного в приложении к Статье 18, параграф 2, в производство и обладание такими изображениями с их согласия и только для их собственного использования.*

4) Каждая сторона может оставить за собой право не применять, полностью или частично, параграф 1f).

Охватываемые действия

Положение основано на Статье 9 Конвенции о киберпреступности и потому в большой степени сравнимо с данным положением[1121]. Главным отличием является то, что Конвенция о киберпреступности стремится преследовать судебным порядком действия, связанные с информационными услугами и услугами связи ("производство детской порнографии с целью ее распространения через компьютерную систему"), а Конвенция по защите детей в основном следует более широкому подходу ("производство детской порнографии") и даже включает действия, не связанные с компьютерными системами.

Несмотря на сходство с учетом охватываемых действий, Статья 20 Конвенции по защите прав детей содержит одно деяние, не охватываемое Конвенцией. На основе Статьи 20, в рамках параграфа 1f) Конвенции по защите детей судебным порядком преследуется действие по получению доступа к детской порнографии посредством компьютера. Это позволяет органам охраны правопорядка преследовать злоумышленников, когда они могут доказать, что злоумышленник открыл веб-сайты с детской порнографией, но не могут доказать, что злоумышленник загружал материалы. Такие трудности при сборе доказательств возникают, например, когда преступник использует технологию шифрования на своих носителях хранения для защиты загруженных файлов[1122]. В Пояснительном Отчете к Конвенции по правам ребенка указывается, что это положение также должно применяться, когда преступник рассматривал

[1121] *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1122] Regarding the challenges related to the use of encryption technology see above: Chapter 3.2.13. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology See: *Wolak/ Finkelhor/ Mitchell*, "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study", 2005, page 9, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

изображения с детской порнографией в режиме онлайн, не загружая их[1123]. В целом открытие веб-сайта автоматически запускает процесс загрузки – часто без ведома пользователя[1124]. Поэтому случай, упомянутый в Пояснительном отчете, применим только когда не производится фоновая загрузка.

Типовой закон Содружества

Подход, схожий со Статьей 9 Конвенции о киберпреступности можно найти в Разделе 10 типового закона Содружества[1125] 2002 года.

> ***Раздел 10***
>
> *1) Лицо, умышленно совершающее любое из перечисленных действий:*
>
> *a) публикация детской порнографии посредством компьютерной системы; или*
>
> *b) производство детской порнографии с целью ее публикации посредством компьютерной системы; или*
>
> *c) обладание детской порнографией на компьютерной системе или на компьютерном носителе хранения данных; признается преступлением, караемым, по приговору, тюремным заключением на срок, не превышающий [срок], или штрафом, не превышающим [размер], или и тем и другим[1126].*
>
> *2) Оправданием в обвинениях в преступлении в рамках параграфа 1 a) или 1 (c) является то, если лицо установило, что детская порнография добросовестно использовалась только для научных, исследовательских, медицинских или правоохранительных целей[1127].*
>
> *3) В данном разделе:*
>
> *"детская порнография" включает в себя материалы, изображающие:*
>
> *a) несовершеннолетнего, участвующего в действиях с сильным сексуальным содержанием; или*
>
> *b) лицо, кажущееся несовершеннолетним, вовлеченное в действия с сильным сексуальным содержанием; или*
>
> *c) реалистичные изображения несовершеннолетнего, участвующего в действиях с сильным сексуальным содержанием.*
>
> *"несовершеннолетний" означает лицо моложе [x] лет.*
>
> *"публикация" включает в себя:*
>
> *a) распространение, передачу, раздачу, обращение, доставку, демонстрацию, сдачу для получения прибыли, обмен, бартер, продажу или предложение о продаже, сдача внаем или*

[1123] See Explantory Report to the Convention on the Protection of Children, No. 140.

[1124] The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser the information can be downloaded to cache and temp files or are just stored in the RAM memory of the computer. Regarding the forensic aspects of this download see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180, available at: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[1125] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1126] Official Notes:
NOTE: The laws respecting pornography vary considerably throughout the Commonwealth. For this reason, the prohibition in the model law is limited to child pornography, which is generally the subject of an absolute prohibition in all member countries. However a country may wish to extend the application of this prohibition to other forms of pornography, as the concept may be defined under domestic law.
NOTE: The pecuniary penalty will apply to a corporation but the amount of the fine may be insufficient. If it is desired to provide a greater penalty for corporations, the last few lines of subsection (1) could read: "commits an offence punishable, on conviction: (a) in the case of an individual, by a fine not exceeding [amount] or imprisonment for a period not exceeding [period]; or (b) in the case of a corporation, by a fine not exceeding [a greater amount].

[1127] Official Note:
NOTE: *Countries may wish to reduce or expand upon the available defences set out in paragraph 2, depending on the particular context within the jurisdiction. However, care should be taken to keep the defences to a minimum and to avoid overly broad language that could be used to justify offences in unacceptable factual situations.*

предложение о сдаче, предложение любым другим способом, предоставление доступности любым способом; или

b) обладание в собственности или хранении, или под контролем, с целью совершения действий, описанных в параграфе a); или

c) печать, фотографирование, копирование или тиражирование любым другим способом, похожим или отличным по виду или природе, для целей совершения действий, описанных в параграфе a).

Основным отличием от Конвенции о киберпреступности является то, что типовой закон Содружества не дает четкого определения термина несовершеннолетний и оставляет определение этого возрастного предела на усмотрение Государств-Членов.

В неофициальном[1128] проекте Стэнфордской Конвенции 1999 года нет положения, преследующего судебным порядком обмен детской порнографией через компьютерные системы. Разработчики Конвенции указали, что в целом ни один вид высказываний или публикаций не должен преследоваться судебным порядком в рамках Стэнфордского проекта[1129]. Учитывая разницу в национальных подходах, составители Конвенции оставили за государствами право решения об этом аспекте судебного преследования[1130].

6.1.8 Агрессивные высказывания, расизм

Не во всех странах агрессивные высказывания преследуются судебным порядком[1131].

Конвенция о киберпреступности

Так как стороны, подписавшие Конвенцию о киберпреступности, не смогли придти к соглашению[1132] по общей позиции касательно судебного преследования таких материалов, положения, относящиеся к данной теме, были включены в отдельный Первый Протокол к Конвенции о киберпреступности[1133].

Положение

Статья 3 – Распространение расистских и связанных с ксенофобией материалов через компьютерные системы

1 Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное создание, без права на это, следующих действий: распространение или предоставление широкого доступа к расистским материалам и материалам ксенофобского содержания через компьютерную систему.

[1128] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1129] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1130] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1131] For an overview of hate speech legislation, see the database provided at: http://www.legislationline.org.

[1132] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime No. 4: "The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention."

[1133] Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

2 Сторона может оставить за собой право не применять уголовной ответственности к деянию, как указано в параграфе 1 данной статьи, когда материал, как указано в Статье 2, параграф 1, защищает, содействует или провоцирует различие того, что не связано с ненавистью или насилием, при условии, что доступны другие эффективные средства.

3 Не взирая на параграф 2 данной статьи, сторона может оставить право не применять параграф 1 к таким случаям дискриминации, для которых из-за устоявшихся принципов в ее национальной правовой системе, относящихся к свободе выражения, нельзя найти эффективных средств, как сказано в упомянутом параграфе 2.

Статья 4 – Угрозы, вызванные расизмом и ксенофобией

Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное совершение, без права на это, следующих действий:

передача через компьютерную систему угрозы совершения тяжкого уголовного преступления, как указывается во внутригосударственном законе, i) в отношении лиц по причине их принадлежности к группе, отличающейся по расе, цвету, происхождению или национальной или этнической принадлежности, или по религиозным воззрениям, если эта принадлежность используется как повод для любого их таких факторов, или ii) группе лиц, отличающейся по любой из этих характеристик.

Статья 5 – Оскорбления, вызванные расизмом и ксенофобией

Каждая Сторона принимает законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное совершение, без права на это, следующих действий:

публичные оскорбления через компьютерную систему, i) лиц по причине их принадлежности к группе, отличающейся по расе, цвету, происхождению или национальной или этнической принадлежности, или по религиозным воззрениям, если эта принадлежность используется как повод для любого их таких факторов, или ii) группе лиц, отличающейся по любой из этих характеристик.

2 Либо сторона может:

a) потребовать, чтобы преступление, относящееся к параграфу 1 данной статьи, имело такие последствия, чтобы лицо или группа лиц, относящиеся к параграфу 1, были беззащитны перед ненавистью, презрению или насмешкам; или

b) оставить за собой право не применять, полностью или частично, параграф 1 данной статьи.

Статья 6 – Отрицание, существенное преуменьшение, принятие или оправдание геноцида или преступлений против человечества

Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное создание, без права на это, следующих действий:

публичное распространение или создание доступа любым другим способом через компьютерную сеть материалов, которые отрицают, существенно преуменьшают, принимают или оправдывают действия, заключающиеся в геноциде или преступлениях против человечества, как указывает международное право и рассматривающиеся таким образом окончательными и обязательными решениями Международного военного трибунала, учрежденного Лондонским соглашением 8 августа 1945 года, или любым другим международным судом, учрежденного равнозначным международным органом, и чьи полномочия принимаются данной стороной.

2 Либо сторона может:

a) потребовать, чтобы отрицание или существенное преуменьшение, относящиеся к параграфу 1 данной статьи, совершались с намерением разжечь ненависть, дискриминацию или насилие против любого человека или группы лиц, основываясь на их расе, цвету, происхождению или национальной или этнической принадлежности, так и по религиозным воззрениям, если используется в качестве повода для любого из таких факторов, или в ином случае;

b) оставить за собой право не применять, полностью или частично, параграф 1 данной статьи.

Одной из главных проблем, связанных с положением, преследующим судебным порядком материалы ксенофобного содержания, является сохранение баланса между гарантией свободы слова[1134], с одной стороны, и предотвращением ущемления прав человека или групп, с другой стороны. Без углубления в детали, трудности при обсуждении Конвенции о киберпреступности[1135] и статус подписей/ратификаций Дополнительного протокола[1136] показывают, что процессу гармонизации мешает разное понятие защиты свободы слова[1137]. Особенно учитывая общие принципы двойной преступности[1138], отсутствующая гармонизация ведет к проблемам в усилении в случаях, когда затрагиваются международные вопросы[1139].

Проект Стэнфордской Конвенции

В неофициальном[1140] проекте Стэнфордской Конвенции 1999 года нет положения, преследующего судебным порядком агрессивные высказывания. Составители Конвенции указали, что в целом ни один вид высказываний или публикаций не должен преследоваться в уголовном порядке в рамках Стэнфордского проекта[1141]. Учитывая разные национальные подходы, составители Конвенции оставили на усмотрение государств право решения об этом аспекте судебного преследования[1142].

[1134] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

[1135] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

[1136] Regarding the list of states that signed the Additional Protocol see above: Chapter 5.1.4.

[1137] Regarding the difficulties related to the jurisdiction and the principle of freedom of expression see as well: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: http://www.coe.int/t/e/human_rights/ecri/1-EComputer Law Review International/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/Computer Law Review International(2000)27.pdf.

[1138] Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1139] Regarding the challenges of international investigation see above: Chapter 3.2.5 and *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf;

[1140] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1141] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1142] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

6.1.9 Религиозные преступления

Объем защиты религиозных воззрений и их символов отличается в каждой стране[1143].

Конвенция о киберпреступности

Обсуждение этой темы между сторонами Конвенции о киберпреступности встретило те же трудности, которые отличали материалы, связанные с ксенофобией[1144]. Однако страны, которые обсуждали положения Первого Дополнительного протокола к Конвенции о киберпреступности, согласились добавить религию к предмету защиты в двух положениях.

Положения

> ***Статья 4 – Угрозы, вызванные расизмом и ксенофобией***
>
> *Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное создание, без права на это, следующих действий:*
>
> *передача через компьютерную систему угрозы совершения тяжкого уголовного преступления, как указывается во внутригосударственном законе, i) в отношении лиц по причине их принадлежности к группе, отличающейся по расе, цвету, происхождению или национальной или этнической принадлежности, или по религиозным воззрениям, если используется в качестве повода для любого их таких факторов, или ii) группе лиц, отличающейся по любой из этих характеристик.*
>
> ***Статья 5 – Оскорбления, вызванные расизмом и ксенофобией***
>
> *Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву преднамеренное совершение, без права на это, следующих действий:*
>
> *публичные оскорбления через компьютерную систему, i) лиц по причине их принадлежности группе, отличающейся по расе, цвету, происхождению или национальной или этнической принадлежности, так и по религиозным воззрениям, если используется в качестве повода для любого их таких факторов, или ii) группе лиц, отличающейся по любой из этих характеристик.*

Хотя эти два положения рассматривают религию, как характеристику, они не защищают религиозные воззрения или символы при помощи судебного преследования. Положения преследуют судебным порядком угрозы и оскорбления людей из-за того, что они принадлежат к некоторой группе.

Примеры из национальных законодательств

Некоторые страны идут дальше этого подхода и преследуют судебным порядком последующие действия, связанные с религиозными вопросами. Например Уголовный кодекс Пакистана содержит Разделы с 295B и 295C.

> ***295-B*** *Осквернение и пр. Священного Корана: любой, кто умышленно оскверняет, портит или оскорбляет список Священного Корана или цитаты из него, или использует его любым непочтительным видом или для незаконных целей, будет подвергнут пожизненному заключению.*
>
> ***295-C*** *Применение оскорбляющих замечаний в отношении Святого Пророка: любой, на словах, устно или письменно, или изображением, или любыми измышлениями, намеками или инсинуациями, прямо или косвенно, оскверняющий имя Святого Пророка Мохаммеда (да пребудет над ним мир), будет подвергнут смерти, или пожизненному заключению, или также подвергнут штрафу.*

[1143] Regarding the legislation on blasphemy, as well as other religious offences, see: "Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred", 2007, available at: http://www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf;

[1144] See above: Chapter 6.1.h as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

Учитывая неопределенность в применении этого положения, проект Уголовного кодекса Пакистана 2006 года по электронным преступлениям содержит два положения, касающиеся преступлений, связанных с интернетом[1145]:

> ***20 Осквернение и пр. списка Священного Корана****: любой, при помощи любой электронной системы или электронного устройства умышленно оскверняющий, портящий или оскорбляющий список Священного Корана или цитаты из него, или использующий его любым непочтительным видом или для незаконных целей, будет подвергнут пожизненному заключению.*
>
> ***21 Применение оскорбляющих замечаний и пр. в отношении Святого Пророка****: любой, при помощи любой электронной системы или электронного устройства на словах, устно или письменно, или изображением, или любыми измышлениями, намеками или инсинуациями, прямо или косвенно, оскверняющий имя Святого Пророка Мохаммеда (да пребудет над ним мир), будет подвергнут смерти, или пожизненному заключению, или также подвергнут штрафу.*

Как и в случае с положениями, преследующими судебным порядком распространение через интернет ксенофобных материалов, одна из главных проблем глобальных подходов к преследованию судебным порядком религиозных преступлений связана с принципом свободы слова[1146]. Как указывалось ранее, разный подход к защите свободы слова является препятствием для процесса гармонизации[1147]. Особенно учитывая общие принципы двойной преступности[1148], недостаток гармонизации ведет к трудностям в усилении, когда затрагиваются международные вопросы[1149].

6.1.10 Незаконные азартные игры

Беспокойство вызывает растущее число веб-сайтов[1150], предлагающих незаконные азартные игры, так как они могут использоваться для обхода запрета на азартные игры, существующие в некоторых странах[1151]. Если услуги управляются из мест, где азартные онлайновые игры не запрещены, то для стран, которые преследуют судебным порядком работу Интернет-казино, будет трудно помешать своим гражданам пользоваться этими услугами[1152].

[1145] The draft law was not in power, at the time this publication was finalised.

[1146] Regarding the principle of freedom of speech see: *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; Regarding the importance of the principle with regard to electronic surveillance see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol 15, No. 2, 2002, page 530 et seqq; Vhesterman, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 et. seq., available at: http://www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: http://www.fas.org/sgp/crs/misc/95-815.pdf.

[1147] Regarding the difficulties related to the jurisdiction and the principle of freedom of expression see as well: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: http://www.coe.int/t/e/human_rights/ecri/1-EComputer Law Review International/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ Computer Law Review International(2000)27.pdf.

[1148] Dual criminality exists if the offence is a crime under both the requestor and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: "United Nations Manual on the Prevention and Control of Computer-Related Crime", 269, available at http://www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, "Harmonizing National Legal Approaches on Cybercrime", 2005, page 5, available at: http://www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1149] Regarding the challenges of international investigation see above: Chapter 3.2.f and *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension", in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf;

[1150] The 2005 eGaming data report estimates the total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: http://www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm. Regarding the number of licensed Internet websites related to Internet gambling in selected countries, see: "Internet Gambling – An overview of the Issue", GAO-03-89, page 52, available at: http://www.gao.gov/new.items/d0389.pdf; Regarding the total numbers of Internet gambling websites see: *Morse*, "Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion", page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf

[1151] For an overview of different national Internet gambling legislation, see: "Internet Gambling – An overview of the Issue", GAO-03-89, page 45 et seqq., available at: http://www.gao.gov/new.items/d0389.pdf.

[1152] Regarding the situation in the People's Republic of China, see for example: "Online Gambling challenges China's gambling ban", available at: http://www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

Примеры из национальных законодательств

В Конвенции о киберпреступности нет запрета на азартные онлайновые игры. Примером национального подхода к данному вопросу служит Раздел 284 Уголовного Кодекса Германии:

Пример

> ***Раздел 284 Незаконная организация азартных игр***
>
> *1) Лицо, которое без разрешения органов государственной власти, открыто организует или проводит азартные игры, или предоставляет оборудование для них, карается тюремным заключением на срок до двух лет или штрафом.*
>
> *2) Азартные игры в клубах или частных вечеринках, где регулярно организовываются азартные игры, считаются открыто организованными.*
>
> *3) Лицо, которое в случаях, подпадающих под подраздел 1), действует:*
>
> *профессионально; или*
>
> *2 в качестве участника группы, организованной для постоянного совершения таких действий, карается тюремным заключением на срок от трех месяцев до пяти лет.*
>
> *4) Лицо, которое привлекает к азартным играм (подразделы 1) и 2)), карается тюремным заключением на срок до одного года или штрафом.*

Это положение предназначено для ограничения риска зависимости[1153] от игры, путем определения процедур для организации таких игр[1154]. Она не ориентирована явно на азартные игры в интернете, но включает их[1155]. С этой стороны она преследует судебным порядком незаконные азартные игры, проводящиеся без разрешения уполномоченных органов власти. Дополнительно она преследует законным порядком любого, кто умышленно предоставляет оборудование, которое затем используется для незаконных азартных игр[1156]. Данное судебное преследование выходит за рамки последствий от помощи и соучастия, так как преступники могут иметь более строгие меры наказания[1157].

Во избежание уголовного расследования операторы веб-сайтов с незаконными азартными играми могут физически переносить свою деятельность[1158] в страны, где незаконные азартные игры не преследуются судебным порядком[1159]. Такой перенос в места представляет собой сложную задачу для органов охраны правопорядка, так как факт того, что сервер находится за пределами некоторой страны[1160], в целом не влияет на возможность пользователя получить к нему доступ внутри страны[1161]. Для того чтобы улучшить возможности борьбы органов охраны правопорядка против незаконных азартных игр, правительство

[1153] Regarding the addiction see: *Shaffer*, Internet Gambling & Addiction, 2004 , available at: http://www.ncpgambling.org/media/pdf/eapa_flyer.pdf ; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: https://www.european-lotteries.org/data/info_130/Wood.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: http://www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, http://www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

[1154] See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

[1155] See *Thumm*, Strafbarkeit des Anbietens von Internetglueckspielen gemaess § 284 StGB, 2004.

[1156] Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which did not know that their services were abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

[1157] For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously the criminalisation is limited to those cases where the offender is intentionally making the equipment available.

[1158] This is especially relevant with regard to the location of the server.

[1159] Avoiding the creation of those safe havens is a major intention of harmonisation processes. The issue of safe havens was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out that: '*states should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies*". The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "*There must be no safe havens for those who abuse information technologies*".

[1160] With regard to the principle of sovereignty changing the location of a server can have a great impact on the ability of the law enforcement agencies to carry out an investigation. National Sovereignty is a fundamental principle in International Law. See *Roth*, 'state Sovereignty, International Legality, and Moral Disagreement", 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

[1161] Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene see above: Chapter 3.2.6 and Chapter 3.2.7.

Германии расширило судебное преследование до пользователей[1162]. Основываясь на Разделе 285, органы охраны правопорядка могут преследовать пользователей, которые участвуют в незаконных азартных играх и могут начинать расследования, даже если операторы азартных игр не могут быть наказаны, так как они находятся вне пределов Германии:

> ***Раздел 285 Участие в незаконных азартных играх***
>
> *Любой, принимающий участие в открытых азартных играх (Раздел 284), карается тюремным заключением на срок до шести месяцев или штраф до ста восьмидесяти дневных ставок оплаты труда.*

Если преступник использует сайты с азартными играми для действий по отмыванию денег, то идентификация преступников часто затруднена[1163]. Примером служит подход[1164] для предотвращения незаконных азартных игр и действий по отмыванию денег, принятый в законе Соединенных Штатов по усилению борьбы с незаконными азартными играми через интернет 2005 года[1165].

> ***5363 Запрет на принятие любых финансовых инструментов для незаконных азартных игр через интернет***
>
> *Никто, участвующий в предприятиях по совершению ставок или заключению пари, не может умышленно принимать, для участия другого лица в незаконных азартных играх через интернет*
>
> *1) кредит или проценты от кредита, принадлежащие другому лицу или от имени такого другого лица, включая кредит, полученный по кредитной карте;*
>
> *2) перевод с электронного счета, или счетов переданных от имени или через предприятия по пересылке денег, или процентов от перевода с электронного счета или услуг по пересылке денег, от или от имени такого другого лица;*
>
> *3) любые чеки, траты или подобные инструменты, подписанные таким другим лицом или от его имени и подписанные или оплачиваемые через любые финансовые организации; или*
>
> *4) проценты от любого другого вида финансовых сделок, как Секретарь может предписать по правилам, которые используют финансовые организации в качестве плательщика или финансового посредника от лица или для пользы такого другого лица.*
>
> ***5364 Правила и процедуры для определения и предотвращения запрещенных сделок***
>
> *До окончания периода в 270 дней с начала даты принятия этого параграфа Секретарь после консультаций с Советом управляющих федеральной резервной системы и Генеральным Прокурором должен установить правила, требующие от каждой отмеченной платежной системы и всех ее участников, определять и предотвращать запрещенные сделки при помощи создания правил и процедур, правильно составленных для определения и предотвращения запрещенных сделок любым из перечисленных способов:*
>
> *1) Создание правил и процедур, которые*

[1162] For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

[1163] Regarding the vulnerability of Internet gambling to money laundering, see: "Internet Gambling – An overview of the Issue", GAO-03-89, page 5, 34 et seq., available at: http://www.gao.gov/new.items/d0389.pdf.

[1164] Regarding other recent approaches in the United States see *Doyle*, Internet Gambling: A Sketch of Legislative Proposals in the 108th Congress, CRS Report for Congress No. RS21487, 2003, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-4047: *Doyle*, Internet Gambling: Two Approache sin the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: http://www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

[1165] For an overview of the law, see: *Landes*, "Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation", available at: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, "Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed", 2006, available at: http://www.gamblingandthelaw.com/columns/2006_act.htm. *Shaker*, Americas's Bad Bet: How the Unlawful Internet Gambling Enforcement act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII, page 1183 et. seq., available at: http://law.fordham.edu/publications/articles/600flspub8956.pdf.

A) позволяют платежной системе и любому лицу, участвующему в платежной системе, определять запрещенные сделки посредством кодов в сообщениях авторизации или иными способами; и

B) блокируют запрещенные сделки, определенные в результате применения правил и процедур, разработанных в соответствии с подпараграфом A);

2) Создание правил и процедур, предотвращающих принятие продуктов услуг платежных систем, относящихся к запрещенным сделкам.

b) При создании правил в рамках подраздела a) Секретарь должен

1) определить виды правил и процедур, включая неисключительные правила, которые должны считаться достаточными, чтобы разумно применяться для определения, блокирования или предотвращения принятия продуктов услуг, учитывая каждый вид запрещенной сделки;

2) для расширения практического применения разрешить любому участнику платежной системы выбирать между альтернативными способами определения и блокирования, или, в ином случае, предотвращения принятия продуктов услуг платежных системы или участника, имеющих отношение к запрещенным сделкам; и

3) учитывать освобождение запрещенных сделок от любых требований, налагаемых в рамках таких правил, если Секретарь решит, что они недостаточно практичны для определения и блокирования, или, иначе, предотвращения таких сделок.

c) Должно предполагаться, что поставщик финансовых сделок соответствует правилам, установленным в рамках подраздела a), если

1) такое лицо полагается и соответствует правилам и процедурам обозначенной платежной системы, членом или участником оно является, чтобы

A) определять и блокировать запрещенные сделки; или

B) другими способами предотвращать принятие продуктов или услуг платежной системы, члена или участника, связанных с запрещенными сделками; и

2) эти правила и процедуры обозначенной платежной системы соответствовали требованиям правил, установленных в рамках подраздела a).

d) Лицо, к которому применяются правила, установленные или распоряжения, выпущенные в рамках данного параграфа и блокировки, или иные отказы в выполнении передачи,

1) которая является запрещенной сделкой;

2) что такое лицо достоверно считается совершающим запрещенную сделку; или

3) как член обозначенной платежной системы, в зависимости от правил и процедур платежной системы, в попытках соответствовать правилам, установленным в рамках подраздела (a), не должен помогать ни одной стороне в таких действиях.

e) Требования этого раздела будут усиливаться только Федеральными органами функционального регулирования и Федеральной комиссией по торговле, способами, указанными в разделе 505 a) закона Грамма-Лича-Блайли.

5366 Уголовные санкции

a) Любой, нарушивший раздел 5363, будет оштрафован в рамках Статьи 18 или подвергнут тюремному заключению на срок не более 5 лет, или и то и другое.

b) По приговору лица в рамках данного раздела суд может ввести постоянный запрет для данного лица совершать, получать или любым другим способом делать ставки или пари или отправлять, получать или привлекать информацию, способствующую совершению ставок или пари.

Задачей этого закона является решение проблем и угроз обусловленных (зарубежными) азартными играми через интернет[1166]. Он содержит два важных правила: первое – запрет на принятие любым лицом, участвующим в предприятии, связанном со ставками и пари, любого финансового инструмента для незаконных азартных игр через интернет. Это положение не регулирует действий, предпринимаемых пользователем сайтов для незаконных азартных игр через интернет или финансовыми учреждениями[1167]. Нарушение данного запрета может привести к уголовному наказанию[1168]. Дополнительно Закон требует от Секретаря Казначейства и Совета директоров Федеральной резервной системы установить правила, требующие от поставщиков финансовых сделок определять и блокировать посредством любых приемлемых правил и процедур запрещенные сделки, связанные с незаконными азартными играми через интернет. Это втрое правило касается не только лиц, участвующих в компаниях по совершению ставок и пари, но в целом всех финансовых учреждений. В отличии от принятия финансовых инструментов для незаконных азартных игр через интернет лицом, участвующим в предприятиях по совершению ставок и пари, финансовые учреждения в целом не подвергаются уголовному преследованию. Учитывая международное воздействие правил, в настоящее время с Генеральным соглашением по торговле услугами (GATS)[1169] расследуются[1170] возможные конфликты.

6.1.11 Клевета и оскорбление

Клевета и публикация ложной информации не являются деяниями, совершаемыми только в сетях. Но как указывалось ранее, абстрактными параметрами, поддерживающими это деяние, служат возможность анонимного общения[1171] и логистических вызовов, связанных с большим массивом информации[1172], доступной через интернет.

Широко обсуждается вопрос, требует ли клевета судебного преследования[1173]. Опасения касательно судебного преследования клеветы особо связаны с возможным противоречием с принципам "свободы слова". Поэтому некоторые организации потребовали замены уголовного преследования клеветы[1174]. Специальный Докладчик ООН по свободе мнений и их выражения и Представитель ОБСЕ по свободе средств массовой информации указали, что:

> *"Уголовно-наказуемая клевета не является позволительным ограничением свободы выражения; все уголовные законы о клевете должны быть отменены и заменены, где это необходимо, соответствующими гражданскими законами о клевете*[1175]*"*.

[1166] *Landes*, "Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation", available at: http://www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, "Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed", 2006, available at: http://www.gamblingandthelaw.com/columns/2006_act.htm.

[1167] *Rose*, "Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed", 2006, available at: http://www.gamblingandthelaw.com/columns/2006_act.htm.

[1168] Based on Sec. 5366 the criminalisation is limited to the acceptance of financial instruments for unlawful Internet gambling

[1169] General Agreement on Trade in Services (GATS) – with regard to the United States Unlawful Internet Gambling Enforcement Act especially Articles XVI (dealing with Market Access) and XVII (dealing with National Treatment) could be relevant.

[1170] See "EU opens investigation into US Internet gambling laws ", EU Commission press release, 10.03.2008, available at: http://ec.europa.eu/trade/issues/respectrules/tbr/pr100308_en.htm; *Hansen*, EU investigates DOJ internet gambling tactics, The Register, 11.03.2008, available at: http://www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.

[1171] See above: Chapter 3.2.l.

[1172] See above: Chapter 3.2.2.

[1173] See for example: Freedom of Expression, Free Media and Information, Statement of Mr. *McNamara*, United States Delegation to the OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf; Regarding the development of the offence see: Walker, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: http://www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf. Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: http://www.article19.org/pdfs/standards/definingdefamation.pdf. *Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts" Washington University Law Review, 2006, page 1157 et. seq., available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 et seq., available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol 84, 2006, page 1187 et. seq., available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[1174] See for example the Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002. For more information see: http://www.osce.org/documents/rfm/2004/10/14893_en.pdf. See in addition the statement of the representative on Freedom of the Media, Mr. Haraszti at the Fourth Winder Meeting of the OSCE Parliamentary Assembly at the 25th of February 2005:

[1175] Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002. For more information see:

Несмотря на это, некоторые страны[1176] приняли положения уголовного законодательства, преследующие судебным порядком как клевету, так и публикацию ложной информации. Необходимо подчеркнуть, что даже внутри стран, преследующих судебным порядком клевету, количество дел сильно различается. Например, в Соединенном Королевстве в 2004 году не было ни одного дела, а в 2005 году в клевете был обвинен только один подозреваемый[1177]. В 2006 году в Германии было зарегистрировано 187 527 преступлений, связанных с клеветой[1178]. В Конвенции о киберпреступности, типовом законе Содружества и проекте Стэнфордской Конвенции нет положений, напрямую касающихся этих деяний.

Примеры из национального законодательства

Одним примером положения уголовного кодекса, касающегося клеветы, является Раздел 365 Уголовного Кодекса Квинсленда (Австралия). В Квинсленде в 2002 году принята Поправка к закону об уголовной ответственности за клевету 2002 года, которая восстановила уголовную ответственность за клевету[1179].

Положение

> ***365 Уголовно-наказуемая клевета***[1180]
>
> *1) Любое лицо, без законного основания публикующее материал, клевещущий на другого живущего человека (известного человека) –*
>
> *a) зная, что материал ложен или не обращая внимания на правдивость или ложность информации; и*
>
> *b) намереваясь причинить серьезный ущерб известному человеку или любому другому человеку, или не обращая внимания на то, будет причинен серьезный ущерб известному человеку или любому другому человеку; совершает проступок. Максимальное наказание – 3 года тюрьмы.*
>
> *2) При рассмотрении преступления, определенного в этом разделе, обвиняемый имеет законное оправдание за публикацию клеветнического материала об известном человеке только, и единственно, если подраздел (3) применяется.* […]

Другой пример судебного преследования клеветы – Раздел 185 Уголовного Кодекса Германии:

Положение

> ***Раздел 185 Оскорбление***
>
> *Оскорбление должно караться тюремным заключением на срок до одного года или штрафом, и, если оскорбление связано с актом насилия, тюремным заключением на срок до двух лет или штрафом.*

---

http://www.osce.org/documents/rfm/2004/10/14893_en.pdf.

European Convention of Human Rights and the constitutional principle of freedom of expression — the cornerstone of all modern democracies — the European Court of Human Rights, the United States Supreme Court, the UN Rapporteur on Freedom of Opinion and Expression, the OAS Special Rapporteur on Freedom of Expression, the OSCE Representative on Freedom of the Media, constitutional and supreme courts of many countries, and respected international media NGOs have repeatedly stated that criminal defamation laws are not acceptable in modern democracies. These laws threaten free speech and inhibit discussion of important public issues by practically penalising political discourse. The solution that all of them prefer and propose is to transfer the handling of libel and defamation from the criminal domain to the civil law domain"

[1176] Regarding various regional approaches regarding the criminalisation of defamation see Greene (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: http://www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An "Instrument of Destruction, 2003, available at: http://www.silha.umn.edu/oscepapercriminaldefamation.pdf.

[1177] For more details see the British Crime Survey 2006/2007 published in 2007, available at: http://www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

[1178] See Polizeiliche Kriminalstatistik 2006, available at: http://www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

[1179] The full version of the Criminal Defamation Amendment Bill 2002 is available at: http://www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02_P.pdf; For more information about the Criminal Defamation Amendment Bill 2002 see the Explanatory Notes, available at: http://www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf

[1180] The full text of the Criminal Code of Queensland, Australia is available at: http://www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

Оба положения предназначены не только для описания действий, связанных с интернетом. Их применение не ограничивается определенными способами связи, так что они могут применяться к действиям, совершаемым как в сетях, так и вне сетей.

6.1.12 Спам

Учитывая тот факт, что, как сообщается, до 75%[1181] всех писем электронной почты являются спамом[1182], активно обсуждается необходимость уголовных санкций за рассылку спамовых сообщений[1183]. Национальные законодательные решения, касающиеся спама, различаются между собой[1184]. Одной из главных причин, по которой спам все еще представляет проблему, является то, что технологии фильтрации до сих пор не могут определять и блокировать все спамовые сообщения[1185]. Способы защиты предлагают только ограниченную защиту от нежелательных электронных сообщений.

В 2005 году ОЭСР опубликовала отчет, в котором проанализировано влияние спама на развивающиеся страны[1186]. В отчете указывалось, что представители развивающихся стран часто высказывают мнения, что пользователи интернета их стран сильнее страдают от спама и сетевого злоупотребления. Анализ результатов отчета доказал, что это мнение представителей является верным. Из-за более ограниченных и дорогих ресурсов, спам в развивающихся странах стал более серьезной проблемой, чем в западных странах[1187].

Однако трудности представляет не только идентификация электронных писем со спамом. Очень трудно различить письма, нежелательные для получателя, но отправленные законно, и те, которые отправляются незаконно. Существующая тенденция перехода к передачам на основе компьютеров, включая электронную почту и VoIP, подчеркивает важность защиты связи от атак. Если спам превышает определенный уровень, электронные письма со спамом могут сильно затруднить использование ИКТ и снизить производительность пользователя.

Конвенция о киберпреступности

В Конвенции о киберпреступности спам однозначно не преследуется судебным порядком[1188]. Разработчики предложили, чтобы судебное преследование этих действий было ограничено серьезным и умышленным препятствием связи[1189]. Этот подход не ограничивается нежелательными электронными письмами, а также рассматривает влияние на компьютерную систему или сеть. На основе законного подхода Конвенции о киберпреступности борьба со спамом может основываться только на незаконном искажении компьютерных систем и сетей:

> ***Статья 5 – Искажения системы***

[1181] The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see http://www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mails, see http://spam-filter-review.toptenreviews.com/spam-statistics.html. The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails are spam. See http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf

[1182] For a more information on the phenomenon see above: Chapter 2.5.g. For a precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1183] Regarding the development of spam e-mails, see: *Sunner*, 'security Landscape Update 2007", page 3, available at: http://www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf.

[1184] See "ITU Survey on Anti-Spam Legislation Worldwide, 2005", available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1185] Regarding the availability of filter technology, see: *Goodman,* 'spam: Technologies and Politics, 2003", available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user oriented spam prevention techniques see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam Consumer Perspectives On Spam: Challenges And Challenges, available at: http://www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

[1186] 'spam Issues in Developing Countries", a. Available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

[1187] See 'spam Issues in Developing Countries", Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.

[1188] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1189] Explanatory Report to the Council of Europe Convention on Cybercrime No. 69: "The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ('spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law."

Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы согласно ее внутригосударственному праву квалифицировать в качестве уголовного преступления преднамеренное создание без права на это серьезных помех функционированию компьютерной системы путем ввода, передачи, повреждения, удаления, ухудшения качества, изменения или блокирования компьютерных данных.

Проект Стэнфордской Конвенции

В неофициальном[1190] проекте Стэнфордской Конвенции 1999 года нет положения, преследующего спам судебным порядком. Как и Конвенция по киберпреступности, проект Конвенции считает спам преступлением, только когда нежелательные электронные письма ведут к умышленному искажению системы.

Примеры из национального законодательства

Это ограничивает судебное преследование спама до случаев, когда количество электронных писем со спамом серьезно отражается на производительности компьютерных систем. Электронные письма со спамом влияющие на эффективность торговли, но не обязательно на компьютерную систему, не могут быть наказуемы. Поэтому некоторые страны имеют другой подход. Например, законодательство Соединенных Штатов – 18 U.S.C § 1037[1191].

§ 1037 Обман и схожая деятельность, относящиеся к электронной почте

a) В целом любой, затрагивающий торговлю между штатами или международную торговлю, кто умышленно

1) проникает в защищенный компьютер без санкции и умышленно запускает рассылку множественных коммерческих электронных почтовых сообщений с или с помощью такого компьютера,

2) использует защищенный компьютер для передачи или перенаправления множественных коммерческих электронных почтовых сообщений с намерением обмануть или ввести в заблуждение получателей, или любые услуги доступа в интернет в качестве происхождения таких сообщений,

3) существенно фальсифицирует информацию в заголовке во множественных коммерческих электронных почтовых сообщениях и умышленно начинает рассылку таких сообщений,

4) регистрирует, используя информацию, значительно искажающую личность реального регистрируемого лица, пять или больше электронных почтовых адресов или два или более доменных имени, и умышленно начинает рассылку множественных коммерческих электронных почтовых сообщений с любого сочетания таких адресов или доменных имен, или

5) ложно представляется зарегистрированным лицом или законным представителем интересов зарегистрировавшего лица 5 или больше IP-адресов и умышленно запускает рассылку множественных коммерческих электронных почтовых сообщений с таких адресов,

или вступает в сговор для совершения этого, наказывается в соответствии с подразделом b).

b) Наказания – наказаниями за преступления в рамках подраздела (a) являются

1) штраф в рамках этой статьи, тюремное заключение на срок до 5 лет, или и то и другое, если

[1190] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1191] Regarding the United States legislation on spam see: *Sorkin*, Spam Legislation in the United States, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; Warner, Spam and Beyond: Freedom, Efficiency, and the Regulation of E-Mail Advertising, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Alongi*, Has the U.S. conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 et. seq. , available at: http://www.law.arizona.edu/Journals/ALR/ALR2004/vol462/alongi.pdf; Effectiveness and Enforcement of the CAN-SPAM Act: Report to Congress, 2005, available at: http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

A) преступление совершается для продвижения любого тяжкого преступления по законам Соединенных Штатов или любого штата; или

B) подсудимый ранее привлекался к ответственности в рамках данного раздела или раздела 1030, или закона любого штата за деяние, включающее пересылку множественных коммерческих электронных почтовых сообщений или несанкционированный доступ к компьютерной системе.

Это положение было принято Законом по спаму CAN 2003 года[1192]. Целью закона было создание единого национального стандарта, предназначенного для контроля коммерческих электронных писем[1193]. Он применяется к коммерческим электронным сообщениям, а не к сообщениям, относящимся к сделкам и существующим деловым отношениям. Регулятивный подход требует, чтобы коммерческие электронные сообщения имели указание на навязывание услуг, включая инструкции по уклонению и физический адрес отправителя[1194]. 18 U.S.C. § 1037 преследует судебным порядком отправителей электронных писем со спамом, особенно если они фальсифицируют информацию в заголовке электронных писем для обхода технологий фильтрации[1195]. Дополнительно положение преследует судебным порядком несанкционированный доступ к защищенному компьютеру и запуск рассылки множественных коммерческих электронных почтовых сообщений.

6.1.13 Неправильное использование устройств

Другим серьезным вопросом является доступность программного обеспечения и инструментов аппаратных средств, предназначенных для совершения преступлений[1196]. В отличие от распространения "хакерских устройств" обмен паролями, позволяющими неавторизованным пользователям иметь доступ к компьютерным системам, представляет собой серьезную угрозу[1197]. Доступность и возможные угрозы таких устройств не позволяют преследовать по суду применения этих инструментов только для совершения преступлений. Большинство национальных уголовно-правовых систем содержат некоторые положения, преследующие судебным порядком подготовку и производство этих инструментов дополнительно к "попытке преступления ". Подходом к борьбе с распространением таких устройств является судебное преследование создания инструментов. В целом это судебное преследование, которое обычно сопровождается всесторонним изменением уголовной ответственности, ограничено и касается только самых тяжких преступлений. В частности, в законодательстве ЕС существуют тенденции расширить в проектах законов судебное преследование и применять его к менее тяжким преступлениям[1198].

Конвенция о киберпреступности

Учитывая другие инициативы Совета Европы, составители Конвенции установили независимое уголовное наказание для определенных незаконных деяний в отношении определенных устройств или доступа к данным, для их неправильного использования с целью совершения преступлений против конфиденциальности, целостности и доступности компьютерных систем или данных[1199]:

[1192] For more details about the “Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003” – short: CAN-SPAM act 2003 see: http://www.spamlaws.com/f/pdf/pl108-187.pdf.

[1193] See: *Hamel,* Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?, New Eng. Law Review, 39, 2005, 196 et seq. 325, 327 (2001)).

[1194] For more details see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1195] For more information see: *Wong,* The Future Of Spam Litigation After Omega World Travel v. Mummagraphics, Harvard Journal of Law & Technology, Vol. 20, No. 2, 2007, page 459 et seq., available at: http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech459.pdf.

[1196] “Websense Security Trends Report 2004”, page 11, available at: http://www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; “Information Security - Computer Controls over Key Treasury Internet Payment System”, GAO 2003, page 3, available at: http://www.globalsecurity.org/security/library/report/gao/d03837.pdf. *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[1197] One example of this misuse is the publication of passwords used for access control. Once published, a single password can grant access to restricted information to hundreds of users.

[1198] One example is the EU Framework Decision ABl. EG Nr. L 149, 2.6.2001.

[1199] Explanatory Report to the Council of Europe Convention on Cybercrime No. 71: “To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries“.

Положение

Статья 6 – Неправильное использование устройств

1) Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву в случае совершения преднамеренно и без права на это:

a) производство, продажу, приобретение для использования, импорт, распространение или иные формы предоставления в пользование:

i) устройств, включая компьютерные программы, разработанных или адаптированных, прежде всего для целей совершения какого-либо из правонарушений, предусмотренных выше в Статьях с 2 по 5;

ii) компьютерных паролей, кодов доступа или иных аналогичных данных, с помощью которых может быть получен доступ к компьютерной системе в целом или любой ее части с намерением использовать их с целью совершения какого-либо из правонарушений, предусмотренных в Статьях с 2 по 5; и

b) обладание одним из предметов, упомянутых в пунктах i a) или ii a) выше, с намерением использовать его для совершения каких-либо правонарушений, предусмотренных в Статьях 2–5. Любая Сторона может требовать в соответствии с законом, чтобы условием наступления уголовной ответственности являлось обладание несколькими такими предметами.

2) Настоящая статья не должна толковаться как устанавливающая уголовную ответственность в тех случаях, когда производство, продажа, приобретение для использования, импорт, оптовая продажа или иные формы предоставления в пользование или обладание, упомянутые в параграфе 1 данной статьи, не имеют целью совершение правонарушений, предусмотренных Статьями с 2 по 5 настоящей Конвенции, а связаны, например, с разрешенным испытанием или защитой компьютерной системы.

3) Сторона может зарезервировать за собой право не применять положения параграфа 1 настоящей статьи при условии, что такая оговорка не будет касаться продажи, распространения или иных форм предоставления в пользование предметов, указанных в параграфе 1 a) ii) этой статьи.

Охватываемые предметы

В параграфе 1a) определяются как устройства[1200], предназначенные для совершения и содействия киберпреступлений, так и пароли, дающие доступ к компьютерной системе.

- Термин "устройства" описывает как аппаратные средства, так и программное обеспечение на основе решений для совершения одного из упомянутых преступлений. В Поясняющем Отчете, например, упоминается такое ПО, как вирусные программы, или программы, предназначенные для получения доступа к компьютерным системам[1201].
- "Пароль компьютера, код доступа или схожие данные" в отличие от устройств осуществляют не операции, а дают код доступа. Одним из вопросов, обсуждаемых в данном контексте, является то, охватывает ли это положение публикацию уязвимых мест системы[1202]. В отличие от классических кодов доступа, уязвимые места системы необязательно дают немедленный доступ, а позволяют преступнику использовать уязвимые места для успешных атак на компьютерную систему.

Охватываемые действия

Данная Конвенция преследует судебным порядком широкий спектр действий. Дополнительно к производству она также включает продажу, предоставление для пользования, импорт или другую доступность устройств или паролей. Схожий подход, ограниченный устройствами для обхода технических

[1200] With its definition of „distributing" in the Explanatory Report ('Distribution' refers to the active act of forwarding data to others – Explanatory Report No. 72), the drafters of the Convention restrict devices to software. Although the Explanatory Report is not definitive in this matter, it is likely that it covers not only software devices, but hardware tools as well.

[1201] Explanatory Report to the Council of Europe Convention on Cybercrime No 72.

[1202] See in this context *Biancuzzi*, The Law of Full Disclosure, 2008, available at: http://www.securityfocus.com/print/columnists/466.

мер, можно обнаружить в законодательстве ЕС по гармонизации авторского права[1203], а ряд стран включил похожие положения в свое уголовное законодательство[1204].

- "Распространение" относится к активным действиям по передаче устройств или паролей другим людям[1205].
- "Продажа" относится к деятельности, заключающейся в продаже устройств и паролей за деньги или иное возмещение.
- "Предоставление для пользователя" описывает действия, связанные с активным получением паролей и устройств[1206]. Факт того, что действие предоставления связано с использованием таких устройств, в целом требует, чтобы преступник намеревался представить инструмент для пользования,

---

[1203] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society:

Article 6 – Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

[1204] See for example one approach in the United States legislation:

18 U.S.C. § 1029 (Fraud and related activity in connection with access devices)

(a) Whoever -

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating

$1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)

(1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c)

of this section, or both. […]

[1205] Explanatory Report to the Council of Europe Convention on Cybercrime No 72.

[1206] This approach could lead to a broad criminalization. Therefore Art. 6, Subparagraph 3 Convention on Cybercrime enables the states to make a reservation and limit the criminalization to the distribution, sale and making available of devices and passwords.

выходящего за рамки "обычного" намерения "чтобы он использовался в целях совершения любого преступления, установленного в Статьях с 2 по 5".

Импорт описывает действия по получению устройств и паролей доступа из зарубежных стран[1207]. В результате преступники, импортирующие такие устройства для продажи, могут быть осуждены даже до того, как они их предложат. Учитывая, что предложение таких инструментов преследуется законным порядком только, если оно похоже на использование, возникает вопрос, охватывает ли Статья 6 Конвенции о киберпреступности простой импорт инструментов без намерения их продажи или использования.

"Доступность" относится к действиям, позволяющим другим пользователям получить доступ к предметам[1208]. В Пояснительном Отчете предлагается, чтобы термин "предоставить в распоряжение" также охватывал создание или объединение гиперссылок для облегчения доступа к таким устройствам[1209].

Инструменты двойного применения

В отличие от подхода Европейского Союза к гармонизации авторских прав[1210], это положение применимо не только к устройствам, специально созданным для облегчения действий киберпреступности, Конвенция охватывает также устройства, обычно применяемые для законных целей, в тех случаях, когда особый умысел преступников заключается в совершении киберпреступления. В Пояснительном Отчете составители указали, что ограничения для устройств, созданных только для совершения преступлений, были слишком узкими и могли привести к непреодолимым трудностям приведения доказательств в ходе уголовного преследования, делая это положение практически неприменимым или применимым только в очень редких случаях[1211].

Для обеспечения необходимой зашиты компьютерных систем эксперты применяют и владеют различными программными инструментами, которые могут позволить им использовать правовое применение. Конвенция изучает отношения тремя способами[1212]:

- Она позволяет сторонам в Статье 6, параграф 1b) оставлять за собой право определять минимальное количество таких устройств, находящихся в собственности, прежде чем применять уголовные санкции.
- Кроме того, судебное преследование обладания такими устройствами ограничивается необходимостью умышленного использования этого устройства для совершения преступления, как указано в Статьях с 2 по 5 Конвенции[1213]. В Пояснительном Отчете указывается, что этот особый умысел был включен во "избежание опасности превышения уровня судебного преследования, когда

[1207] Art. 6, Subparagraph 3 Convention on Cybercrime enables the states to make a reservation and limit the criminalization to the distribution, sale and making available of devices and passwords.
[1208] Explanatory Report to the Council of Europe Convention on Cybercrime No 72.
[1209] Explanatory Report to the Council of Europe Convention on Cybercrime No 72: *"This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices"*.
[1210] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society.
[1211] Explanatory Report to the Council of Europe Convention on Cybercrime No 73: The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.
[1212] Regarding the United States approach to address the issue see for example 18 U.S.C. § 2512 (2):
(2) It shall not be unlawful under this section for –
(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or
(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.
[1213] *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

устройства произведены и выставлены на продажу с законными целями, например, для отражения атак на компьютерные системы[1214]".

- Наконец, составители Конвенции однозначно указали в параграфе 2, что инструменты, созданные для санкционированной проверки или для защиты компьютерной системы, не охватываются положением, поскольку в положении описываются только несанкционированные действия.

Судебное преследование обладания

В параграфе 1b) развивается положение, приведенное в параграфе 1a), путем преследования судебным порядком обладания устройствами или паролями, если это связано с намерением совершить преступление. Судебное преследование обладания инструментами вызывает споры[1215]. Статья 6 не ограничивается инструментами, которые предназначены только для совершения преступлений, и противники судебного преследования обеспокоены тем, что судебное преследование обладания такими устройствами может привести к созданию неприемлемых угроз для системных администраторов и экспертов по сетевой безопасности[1216]. Конвенция позволяет сторонам требовать, чтобы прежде, чем начать уголовное преследование, в обладании находилось определенное количество таких предметов.

Субъективная сторона

Так же, как и для всех других преступлений, обозначенных Конвенцией о киберпреступности, Статья 6 требует, чтобы злоумышленник совершал преступление умышленно[1217]. Дополнительно к обычному умыслу, учитывая охватываемые действия, Статьи 6 Конвенции о киберпреступности требует добавления особого умысла для совершения любого преступления, указанного в Статьях 2–5 Конвенции о киберпреступности[1218].

Без права

Так же, как и в обсуждавшихся ранее положениях, эти действия должны совершаться "без права"[1219]. Учитывая опасения, что это положение может использоваться для судебного преследования законных операций инструментов программного обеспечения в рамках самозащиты, составители Конвенции указали, что такие действия не рассматриваются, как совершаемые "без права"[1220].

Ограничения и оговорки

Из-за обсуждений необходимости судебного преследования обладания устройствами Конвенция предложила возможность комплексных оговорок в параграфе 3 Статьи 6 дополнительно к Утверждению 2 параграфа 1b).

[1214] Explanatory Report to the Council of Europe Convention on Cybercrime No 76: "Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'."

[1215] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, Page 731.

[1216] See, for example, the World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: http://www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: http://www.out-law.com/page-1217.

[1217] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1218] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76.

[1219] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1220] Explanatory Report to the Council of Europe Convention on Cybercrime No 77.

Если Сторона применяет оговорку, она может исключить судебное преследование обладания инструментами и некоторые незаконные действия в рамках параграфа 1a), например, создание таких устройств[1221].

Типовой закон Содружества

Подход, схожий со Статьей 6 Конвенции о киберпреступности, можно найти в Разделе 9 Типового закона Содружества 2002 года[1222].

> ***Раздел 9***
>
> *1) Лицо совершает преступление, если лицо:*
>
> *a) умышленно или по грубой неосторожности без правомерной причины или объяснения производит, продает, представляет в пользование, экспортирует, распространяет или делает доступным иными способами:*
>
> *i) устройство, включая компьютерную программу, предназначенное или адаптированное для совершения преступления в рамках разделов 5, 6, 7 или 8; или*
>
> *ii) компьютерный пароль, код доступа или схожие данные, с помощью которых можно получить доступ ко всей или любой части компьютерной системы;*
>
> *с намерением, чтобы его мог использовать любой человек для совершения преступления в рамках разделов 5, 6, 7 или 8; или*
>
> *b) обладает предметом, упомянутым в подпараграфе i) или ii), с намерением применения любым человеком для совершения преступления в рамках разделов 5, 6, 7 или 8.*
>
> *2) Лицо, признанное виновным в преступлении в рамках данного раздела, подвергается тюремному заключения на срок, до [срок], или штрафу до [сумма], или и тому и другому.*

Главным отличием от Конвенции о киберпреступности является то, что Типовой закон Содружества преследует судебным порядком действия, совершенные по грубой неосторожности. Во время переговоров по дальнейшим поправкам к положению Типового закона Содружества, преследующему судебным порядком, обсуждалось обладание такими устройствами, группа экспертов предложила, чтобы судебным порядком преследовалось обладание больше, чем одним предметом[1223]. Канада предложила схожий подход, не установив точного количества предметов, которое вызывает судебное преследование[1224].

[1221] For more information see: Explanatory Report to the Council of Europe Convention on Cybercrime No 78.

[1222] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1223] Expert Groups suggest for an amendment:
Paragraph 3:
A person who possesses more than one item mentioned in subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6,7 or 8 unless the contrary is proven.
Official Note: S*ubsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

[1224] Canada's suggestion for an amendment:
Paragraph 3:
3) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (i) or (ii), a court may infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8, unless the person raises a reasonable doubt as to its purpose.
Official Note: S*ubsection 3 is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context.*

Проект Стэнфордской Конвенции

В неофициальном[1225] проекте Стэнфордской Конвенции 1999 года содержится положение, преследующее судебным порядком действия, связанные с определенными незаконными устройствами.

> ***Статья 3 – Преступления***
>
> *1 Преступлениями в рамках данной Конвенции считается, когда любое лицо незаконно и умышленно участвует в любом из следующих деяний без законно подтвержденных санкций, разрешений или согласия:*
>
> *[...]*
>
> *e) производит, продает, использует, отправляет по почте или иными способами распространяет любое устройство или программу, предназначенную для совершения любого действия, запрещенного Статьями 3 и 4 данной Конвенции;*

Составители Конвенции указали, что в рамках Стэнфордского проекта ни один вид высказываний или публикаций не должен преследоваться в уголовном порядке[1226]. Единственное сделанное ими исключение относится к незаконным устройствам[1227]. В данном контексте составители подчеркнули, что судебное преследование должно ограничиваться упомянутыми действиями и, например, не охватывать обсуждение уязвимых мест системы[1228].

6.1.14 Подлог с использованием компьютера

Уголовные дела, включающие подлог с использованием компьютера, считаются редкими, так как большинство правовых документов ранее были материальными. После перевода в цифровой формат ситуация изменилась[1229]. Тенденция перевода документов в цифровой формат поддерживается созданием правового базиса для их применения, например, правового подтверждения цифровых подписей. Дополнительно положения, направленные против подлога с использованием компьютера, играют важную роль в борьбе против "фишинга"[1230].

Конвенция о киберпреступности

Большинство уголовно-правовых систем преследуют судебным порядком подлог материальных документов[1231]. Составители Конвенции указали, что догматическая структура национальных правовых

[1225] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1226] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1227] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1228] "Draft thereby makes criminal the knowing and deliberate effort to cause illegal attacks through such distribution, but not discussions of computer vulnerability intended for evaluating." See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1229] See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

[1230] See for example: *Austria*, Forgery in Cyberspace: The Spoof could be on you, University of Pittsburgh School of Law, Journal of Technology Law and Policy, Vol. IV, 2004, available at: http://tlp.law.pitt.edu/articles/Vol5-Austria.pdf.

[1231] See for example 18 U.S.C. § 495:

> *Whoever falsely makes, alters, forges, or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving, or of enabling any other person, either directly or indirectly, to obtain or receive from the United States or any officers or agents thereof, any sum of money; or Whoever utters or publishes as true any such false, forged, altered, or counterfeited writing, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited; or*
>
> *Whoever transmits to, or presents at any office or officer of the United States, any such writing in support of, or in relation to, any account or claim, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited – Shall be fined under this title or imprisoned not more than ten years, or both.*

Or Sec. 267 German Penal Code:

> *Section 267 Falsification of Documents*
>
> *(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or*

походов различна[1232]. Например, одна концепция основывается на аутентичности автора документа, а другая на аутентичности утверждения. Составители решили применять минимальное количество стандартов и защищать безопасность и сохранность электронных данных, создав дополнительное преступление к обычному подлогу с использованием материальных документов для закрытия дыр в уголовном праве, которое может применяться к данных, хранящимся в электронном виде[1233].

Положение

> ***Статья 7 – Подлог с использованием компьютера***
>
> *Каждая Сторона принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву при умышленном совершении и без права на это ввода, изменения, удаления, или сокрытие данных, приводящих к созданию ложных данных с намерением, чтобы они принимались или обрабатывались с законными целями как истинные, вне зависимости от того, могут ли данные быть считанные и поняты напрямую. Стороны могут потребовать, чтобы было намерение обмануть, или похожим образом ввести в заблуждение, прежде, чем начать судебное преследование.*

Охватываемый предмет

Целью подлога с использованием компьютера являются данные, вне зависимости от того, могут ли они читаться и/или пониматься напрямую. Конвенция определяет компьютерные данные[1234], как "любое отражение фактов, информации или концепций в виде, позволяющем обработку в компьютерной системе, включая программы, позволяющие компьютерной системе выполнять действия ". Это положение относится к компьютерным данным не только как предмету одного из упомянутых действий. Дополнительно необходимо, что эти действия приводили к искажению данных.

Статья 7 требует, как минимум в отношении субъективной стороны, чтобы данные представляли собой эквивалент общественных или частных документов. Это значит, что данные должны быть юридически обоснованы[1235]. Подлог данных, которые нельзя использовать для законных целей, этим положением не охватываются.

1) Охватываемые действия:

- "Ввод" данных[1236] должен соответствовать созданию ложного материального документа[1237].
- Термин "изменение" относится к модификации существующих данных[1238]. В Пояснительном Отчете особо указывается на вариации и частичное изменение[1239].

---

uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.
(2) An attempt shall be punishable.
(3) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious cases exists, as a rule, if the perpetrator:
1. acts professionally or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;
2. causes an asset loss of great magnitude;
3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or
4. abuses his powers or his position as a public official.
(4) Whoever commits the falsification of documents professionally as a member of a gang which has combined for the continued commission of crimes under Sections 263 to 264 or 267 to 269, shall be punished with imprisonment from one year to ten years, in less serious cases with imprisonment from six months to five years.

[1232] See Explanatory Report to the Council of Europe Convention on Cybercrime No 82.

[1233] Explanatory Report to the Council of Europe Convention on Cybercrime No 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

[1234] See Art. 1 (b) Convention on Cybercrime.

[1235] Explanatory Report to the Council of Europe Convention on Cybercrime No 84.

[1236] For example by filling in a form or adding data to an existing document.

[1237] See Explanatory Report to the Council of Europe Convention on Cybercrime No 84.

[1238] With regard the definition of "alteration" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

- Термин "сокрытие" компьютерных данных означает действие, затрагивающее доступность данных[1240]. В Пояснительном Отчете составители особо отметили удерживание или сокрытие данных[1241]. Такое действие, например, может проявляться в виде блокирования определенной информации для базы данных во время автоматического создания электронного документа.

- Термин "удаление" соответствует определению термина в Статье 4, охватывающей действия, когда удаляется информация[1242]. Пояснительный Отчет относится только к удалению данных с носителя данных[1243]. Но в обзоре положения однозначно поддерживается более широкое определение термина "удаление". На основе такого расширенного определения это действие может проявляться или в виде удаления всего файла или в виде частичного стирания информации в файле[1244].

Субъективная сторона

Так же, как для всех преступлений, определенных в Конвенции о киберпреступности, Статья 3 требует, чтобы злоумышленник совершал преступление умышленно[1245]. В Конвенции нет определения термина "умышленно". В Пояснительном Отчете составители указали, что определение "умышленно" должно создаваться на национальном уровне[1246].

Без права

Действие по подлогу может преследоваться в рамках Статьи 7 Конвенции, только если оно совершается "без права"[1247].

Ограничения и оговорки

В Статье 7 также предлагается возможность создания оговорки для ограничения судебного преследования, требованием дополнительных элементов, например, намерения обмануть, прежде, чем применять уголовное преследование[1248].

Типовой закон Содружества

В Типовом законе Содружества 2002 года нет положения, преследующего судебным порядком подлог с использованием компьютера[1249].

[1239] See Explanatory Report to the Council of Europe Convention on Cybercrime No 83.
[1240] With regard the definition of 'suppression" in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.
[1241] See Explanatory Report to the Council of Europe Convention on Cybercrime No 83.
[1242] With regard the definition of "deletion" see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.
[1243] See Explanatory Report to the Council of Europe Convention on Cybercrime No 83.
[1244] If only part of a document is deleted the act might also be covered by the term "alteration".
[1245] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1246] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.
[1247] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.
[1248] See Explanatory Report to the Council of Europe Convention on Cybercrime No 85.
[1249] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

Проект Стэнфордской Конвенции

В неофициальном[1250] проекте Стэнфордской Конвенции содержится положение, преследующее судебным порядком действия, относящиеся к фальсифицированным компьютерным данным.

> ***Статья 3 – Преступления***
>
> *1 Преступлениями в рамках данной Конвенции считается, если любое лицо незаконно и умышленно участвует в любом из следующих деяний без законно подтвержденных санкций, разрешения или согласия:*
>
> *[...]*
>
> *b) создает, хранит, изменяет, удаляет, переадресовывает, указывает неверный адрес, подтасовывает или создает помехи данным в киберсистеме с целью и последствиями создания ложной информации для причинения серьезного ущерба людям или собственности;*
>
> *[...]*

Главным отличием от Статьи 7 Конвенции о киберпреступности является то, что Статья 3 1b) не сосредоточена на простой подтасовке данных, а требует помех компьютерной системе. Статья 7 Конвенции о киберпреступности таких действий не требует. Достаточно, чтобы преступник действовал с умыслом, который считался бы или действовал с законными целями, как если бы был аутентичным.

6.1.15 Кража идентичности

Учитывая как освещение в средствах массовой информации[1251] результатов недавних исследований[1252], так и множество юридических и технических публикаций[1253] в этой области, представляется необходимым поговорить о краже идентичности, как массовом явлении[1254]. Несмотря на глобальные аспекты этого явления, не все страны приняли в своих внутренних уголовно-правовых системах положения, преследующие судебным порядком все действия, связанные с кражей идентичности. Комиссия Европейского Союза недавно постановила, что кража идентичности преследуется судебным порядком еще не во всех Государствах – Членах ЕС[1255]. Комиссия выразила свое мнение, где говорится, что "сотрудничество по укреплению законодательства в ЕС будет проходить лучше, когда кража идентичности будет преследоваться судебным порядком во всех Государствах-Членах" и объявила, что вскоре начнет консультации для определения того, достаточно ли такой законодательной деятельности[1256].

[1250] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1251] See for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, available at: http://edition.cnn.com/2006/US/05/18/identity.theft/; Identity Fraud, NY Times Topics, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html; *Stone*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: http://www.iht.com/articles/2007/03/21/business/identity.php.

[1252] See for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[1253] See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: http://www.privacyrights.org/ar/id_theft.htm.

[1254] Regarding the phenomenon of identity theft see above: Chapter 2.7.3.

[1255] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267.

[1256] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267.

Одной из проблем, связанных со сравнением существующих правовых инструментов для борьбы с кражей идентичности, является то, что они очень сильно различаются[1257]. Единственным согласующимся элементом существующих подходов является то, что осуждаемое поведение связано с одним или более из следующих этапов[1258]:

- Этап 1: Действие по получению информации об идентичности;
- Этап 2: Действие обладания или передачи информации об идентичности;
- Этап 3: Действие использования информации об идентичности для совершения преступления.

На основе этих наблюдений созданы два систематических подхода к судебному преследованию кражи идентичности:

- Создание одного положения, которое преследует судебным порядком действия по получению, обладанию и использованию информации, связанной с идентичностью (для совершения преступлений).
- Отдельное судебное преследование как типичных действий, связанных с получением информации об идентичности, например, незаконный доступ, создание и распространение вредоносных программ, подлог с использованием компьютера, информационный шпионаж и искажение информации, так и действий, связанных с обладанием и использованием такой информации, например мошенничество с использованием компьютера.

Пример применения отдельного положения

Наиболее известными примерами применения отдельного приложения являются Статьи 18 U.S.C. § 1028(a)(7) и 18 U.S.C. 1028A(a)(1). Эти положения охватывают широкий спектр преступлений, связанных с кражей идентичности. В рамках этого подхода судебное преследование не ограничивается определенным этапом, а охватывает все три этапа, упомянутые выше. Тем не менее, важно подчеркнуть, что это положение не охватывает все действия, относящиеся к краже идентичности, особенно те, когда действует жертва, а не преступник.

> ***1028 Мошенничество и сходная деятельность в отношении документов, функций аутентификации и информации***
>
> *а) Любой, в обстоятельствах, описанных в подразделе (с) данного раздела*
>
> *1) сознательно и без правовых санкций создает документ, удостоверяющий личность, функцию аутентификации или поддельный документ, удостоверяющий личность;*
>
> *2) сознательно передает документ, удостоверяющий личность, функцию аутентификации или поддельный документ, удостоверяющий личность, сознавая, что этот документ или функция были украдены или созданы без правовой санкции;*
>
> *3) сознательно обладает с целью незаконного применения или передачи пятью или более документами (отличающимися от выпущенных законным образом для использования владельцем), функциями аутентификации или поддельными документами, удостоверяющими личность;*
>
> *4) сознательно обладает с целью незаконного применения или передачи пятью или более документами (отличающимися от выпущенных законным образом для использования владельцем), функциями аутентификации или поддельными документами, удостоверяющими личность с целью и при помощи таких документов или функций обмана Соединенных Штатов;*
>
> *5) сознательно создает, передает или обладает инструментами для создания документов или функций аутентификации с целью использования этих инструментов для создания документов*

[1257] *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 et seq.

[1258] *Gercke*, Internet-related Identity Theft, 2007, available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

или функций аутентификации для создания поддельных документов, удостоверяющих личность, или других инструментов для создания документов или функций аутентификации для соответствующего применения;

б) сознательно обладает документом, удостоверяющим личность, или функцией аутентификации, который является или кажется документом, удостоверяющим личность, или функцией аутентификации в США, который украден или создан без правовой санкции, сознавая, что такой документ или функция украдены или созданы без такой санкции;

7) сознательно передает, обладает или использует без правовой санкции средства для идентификации другого лица с целью совершения, или помощи, или содействия, или связанного с любыми незаконными действиями, составляющими нарушение федерального закона, или которые являются тяжким преступлением в рамках любого применимого местного закона или закона штата; или

8) сознательно торгует ложными или реальными функциями аутентификации для использования в поддельных документах, удостоверяющих личность, инструментах для создания документов или средств идентификации;

будет наказан в соответствии с подразделом b) данного раздела.

1028A Кража идентичности при отягчающих обстоятельствах

а) Преступления

1) В целом любой, кто во время или в связи с любым обвинением в тяжком преступлении, указанном в подразделе c), сознательно передающий, обладающий, или использующий без правовой санкции средства идентификации другого лица будет, дополнительно к наказанию, определяемому за такое преступление, заключен в тюрьму на срок 2 года.

Этап 1

Для того чтобы совершить преступления, относящиеся к краже идентичности, преступник должен получить во владение данные, связанные с идентичностью[1259]. Преследуя судебным порядком "передачу" средств идентификации для совершения преступления, положения преследуют судебным порядком действия, относящиеся к этапу 1 в очень широком смысле[1260]. Из-за того, что эти положения сосредоточены на действиях по передаче, они не охватывают действий, предпринятых преступником до начала процесса передачи[1261]. Такие действия, как отправка сообщений фишинга и создание вредоносных программ, могущих применяться для получения от жертв данных, связанных с идентичностью компьютера, не охвачены 18 U.S.C. § 1028(a)(7) и 18 U.S.C. 1028A(a)(1).

Этап 2

Преследуя судебным порядком обладание с целью совершения преступления, положения опять следуют широкому подходу в отношении действий, связанных со вторым этапом. Это особенно включает в себя обладание информацией, связанной с идентичностью, с целью использования ее позже для одного из обычных преступлений, связанных с кражей идентичности[1262]. Обладание данными, связанными с идентичностью, без намерения их использовать не рассматривается[1263].

[1259] This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data see above *McFadden*, Synthetic identity theft on the rise, Yahoo Finance, 16.05.2007, available at: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1; ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf.

[1260] The reason for the success is the fact that the provisions are focussing on the most relevant aspect of phase 1: the transfer of the information from the victim to the offender.

[1261] Examples for acts that are not covered is the illegal access to a computer system in order to obtain identity related information.

[1262] One of the most common ways the obtained information are used are linked to fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[1263] Further more it is uncertain if the provisions criminalise the possession if the offender does not intent to use them but sell them. The prosecution could in this case in general be based on fact that 18 U.S.C. § 1028 does not only criminalise the possession with the intent to use it to commit a crime but also to aid or abet any unlawful activity.

Этап 3

Преследуя судебным порядком "использование" с целью совершения преступления, положения охватывают действия, связанные с этапом 3. Как упоминалось выше, 18 U.S.C. § 1028(a)(7) не связан с определенным преступлением, например мошенничеством.

Пример применения множества положений

Главным отличием Конвенцией о киберпреступности от применения одного положения, например подхода США, является то, что в Конвенции не определяется отделяет киберпреступление от незаконного применения информации, связанной с идентичностью[1264]. Так же, как в ситуации, относящейся к судебному преследованию получения информации, связанной с идентичностью, Конвенция не охватывает все возможные действия, связанные с незаконным использованием личной информации.

Этап 1

В Конвенции о киберпреступности[1265] содержится несколько положений, преследующих судебным порядком действия по краже идентичности, связанные с интернетом, на первом этапе. Главным образом, это:

- незаконный доступ (Статья 2)[1266];
- незаконный перехват (Статья 3)[1267];
- искажение информации (Статья 4)[1268].

Учитывая разные возможности того, как преступник может получить доступ к данным, необходимо указать, что не все действия, возможные на этапе 1, охвачены. В качестве примера, которое часто относят к этапу 1 кражи идентичности, но в Конвенции о киберпреступности оно не описывается можно привести информационный шпионаж.

Этап 2

Действия, предпринимаемые между получением информации и использованием ее для совершения преступления, довольно трудно учесть в Конвенции о киберпреступности. В частности, невозможно предотвратить рост черного рынка для торговли информацией, связанной с идентичностью, преследуя законным порядком продажу такой информации на основе положений, установленных Конвенцией.

Этап 3

В Конвенции о киберпреступности Совета Европы определяется несколько преступлений, связанных с киберпреступностью. Некоторые такие преступления могут совершаться злоумышленником при помощи информации, связанной с идентичностью. Мошенничество с использованием компьютера является одним из примеров, который часто упоминается в связи с кражей идентичности[1269]. Исследования по краже идентичности указали, что большая часть полученных данных использовалась для мошеннических операций

[1264] See as well: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: http://www.lex-electronica.org/articles/v11-1/ chawki_abdel-wahab.pdf .

[1265] Similar provisions are included in the Commonwealth Model Law and the Draft Stanford Convention. For more information about the Commonwealth model law see: "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Draft Stanford Convention see: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1266] See above: Chapter 6.1.1.

[1267] See above: Chapter 6.1.3.

[1268] See above: Chapter 6.1.4.

[1269] *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: https://www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

с кредитными картами[1270]. Если мошеннические операции с кредитными картами совершаются в режиме онлайн, преступник, скорее всего, будет наказан в рамках Статьи 8 Конвенции о киберпреступности. Другие преступления, которые могут совершаться при помощи информации, связанной с идентичностью, которая была получена ранее, но не упомянуты в Конвенции, в правовых рамках не рассматриваются. В частности, невозможно преследовать использование информации, связанной с идентичностью, для целей сокрытия идентичности.

6.1.16 Мошенничество с использованием компьютера

Мошенничество – это довольно популярное преступление в киберпространстве[1271]. Оно также является и общей проблемой за пределами интернета, поэтому большинство национальных законов содержат положения, устанавливающие судебное преследование таких преступлений[1272]. Однако применение существующих положений в случаях, связанных с использованием интернета, может быть затруднено, так как традиционные национальные уголовно-правовые положения основаны на ложных данных о человеке[1273]. Во многих случаях мошенничество, совершенное через интернет, это фактически действия компьютерной системы, которая реагирует на действия преступника. Если традиционные уголовные положения, касающиеся мошенничества, не охватывают компьютерные системы, то необходимо обновление национального законодательства[1274].

Конвенция о киберпреступности

Конвенция стремится преследовать судебным порядком любое ненадлежащее действие, в случае обработки данных с целью совершить незаконную передачу собственности, предусмотренной в разделе, относительно мошенничества с использованием компьютера[1275]:

[1270] See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf .

[1271] See above: Chapter 2.7.1.

[1272] Regarding the criminlisation of computer-related fraud in the UK see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 et seq.

[1273] One example of this is Section 263 of the German Penal Code that requires the falsity of a person (mistake). The provision does not therefore cover the majority of computer-related fraud cases:

Section 263 Fraud

(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.

[1274] A national approach that is explicitly address computer-related fraud is 18 U.S.C. § 1030:

Sec. 1030. Fraud and related activity in connection with computers

(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

[1275] Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

Положение

> ***Статья 8 – Мошенничество с использованием компьютера***
>
> *Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы признать в качестве уголовных преступлений в соответствии с ее внутригосударственным правом, когда они совершаются преднамеренно и неправомерно, лишения другого лица его собственности путем:*
>
> *a) любого ввода, изменения, удаления или блокирования компьютерных данных;*
>
> *b) любого вмешательства в функционирование компьютерной системы, мошенническим или бесчестным намерением неправомерного извлечения экономической выгоды для себя или для иного лица.*

Охваченные действия

Статья 8a) содержит перечень наиболее часто совершаемых мошеннических действий с использованием компьютера[1276].

- "Ввод" компьютерных данных охватывает все виды манипуляций ввода, таких как введение неверных данных в компьютер, а также манипуляции с компьютерным программным обеспечением и другие вмешательства в ход обработки данных[1277].
- Термин "изменение" относятся к модификации существующих данных[1278].
- Термин "блокирование" компьютерных данных обозначает действие, которое влияет на доступность данных[1279].
- Термин "удаление" совпадает с определением этого термина в Статье 4, которые охватывает такие действия, при которых информация была удалена[1280].

В дополнение к перечисленным действиям Статья 8 b) содержит общую оговорку: преследовать судебным порядком мошенничество, связанное с "вмешательством в функционирование компьютерной системы". Общая оговорка была добавлена в перечень охватываемых актов, чтобы оставить положение открытым для будущего развития[1281].

Пояснительный Отчет указывает на то, что "вмешательство в функционирование компьютерной системы" охватывает действия, такие как манипуляции с оборудованием, действия подавления распечатки и действия, затрагивающие записи или поток данных, или последовательность, в которой работают программы[1282].

Экономический ущерб

В большинстве национальных уголовных законодательствах уголовные действия должны приводить к экономическому ущербу. Конвенция придерживается аналогичной концепции и ограничивает судебное преследование таких действий, где манипуляции производят прямые экономические или потери собственного имущества других людей, включая деньги, материальные и нематериальные вещи, имеющие экономическую ценность[1283].

Субъективная сторона

Как и другие перечисленные преступления, Статья 8 Конвенции о киберпреступности предусматривает, что преступник действовал умышленно. Это намерение относится к манипуляциям, а также финансовым потерям.

[1276] The drafters highlighted that the four elements have the same meaning as in the previous articles: “To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' in Article 8(a) are supplemented by the general act of 'interference with the functioning of a computer program or system' in Article 8(b). The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles.” See: Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

[1277] Explanatory Report to the Council of Europe Convention on Cybercrime No 86.

[1278] With regard the definition of “alteration” in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No 61.

[1279] With regard the definition of 'suppression” in Art. 4 see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1280] With regard the definition of “deletion” see Explanatory Report to the Council of Europe Convention on Cybercrime No. 61.

[1281] As a result, not only data- related offences, but also hardware manipulations, are covered by the provision.

[1282] Explanatory Report to the Council of Europe Convention on Cybercrime No 87.

[1283] Explanatory Report to the Council of Europe Convention on Cybercrime No 88.

Кроме того, Конвенция требует, чтобы правонарушитель действовал с мошенническим или бесчестным намерением, чтобы получить экономическую или другие выгоды для себя или других[1284]. В качестве примеров действий, исключающих уголовную ответственность в виду отсутствия специального умысла, в Пояснительном Отчете говорится о коммерческой практиках, возникающих в связи с рыночной конкуренцией, что может причинить экономический ущерб одному человеку в интересах другого, но что не производилось с мошенническим или бесчестным намерением[1285].

Без права

Мошенничество с использованием компьютера может преследоваться в соответствии со Статьей 8 Конвенции только в том случае, если оно произошло "без права"[1286]. Данное определение включает требование о том, что экономический эффект должен быть получен без права на это. Составители Конвенции указали, что действия, совершенные в соответствии с действующим договором между пострадавшими лицами, не считаются совершенными без права[1287].

Типовой закон Содружества

Типовой закон Содружества 2002 года не содержит положений о судебном преследовании мошенничества с использованием компьютера[1288].

Проект Стэнфордской Конвенции

Неофициальный[1289] проект Стэнфордской Конвенции 1999 года не содержит положений о судебном преследовании мошенничества с использованием компьютера.

6.1.17 Преступления против авторских прав

Переход с аналогового на цифровое распространение материалов, защищенных авторскими правами, знаменует собой поворотный момент в нарушении авторских прав[1290]. Воспроизводство музыкальных и видео произведений исторически ограничено, так как воспроизводство аналогового источника нередко сопровождается потерей качества при копировании, что в свою очередь, ограничивает возможность

[1284] "The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another."

[1285] The drafters of the Convention point out that these acts are not meant to be included in the offence established by Article 8 - Explanatory Report to the Council of Europe Convention on Cybercrime No 90.

[1286] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1287] Explanatory Report to the Council of Europe Convention on Cybercrime No 90.

[1288] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1289] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1290] Regarding the ongoing transition process, see: "OECD Information Technology Outlook 2006", Highlights, page 10, available at: http://www.oecd.org/dataoecd/27/59/37487604.pdf.

использование копии в качестве источника для дальнейшего воспроизводства. С переходом на цифровые источники качество сохраняется и стало возможным сохранять качество копий неизменно высоким[1291].

Индустрия развлечений ответила введением технических мероприятий (технические средства защиты прав или DRM) для предотвращения воспроизводства[1292], но до сих пор эти меры можно обойти почти сразу после их введения[1293]. Различные программные средства доступны через интернет, что позволяет пользователю копировать музыкальные компакт-диски и диски DVD с фильмами, которые защищены системами DRM. Кроме того, интернет предоставляет неограниченные возможности распространения. В результате нарушение прав интеллектуальной собственности, особенно авторского права, широко распространенными преступлениями в интернете[1294].

Конвенция о киберпреступности

Конвенция включает в себя положение о таких преступлениях, как нарушение авторских прав, которые требуют гармонизации различных положений национальных законодательств:

> ***Статья 10 – Преступления, связанные с нарушением авторских и смежных прав***
>
> *1) Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву нарушения авторского права, как они определены в законодательстве этой Стороны во исполнение обязательств, взятых ею на себя по Парижскому Акту от 24 июля 1971 года, пересматривающему Бернскую Конвенцию об Охране Литературных и Художественных Произведений, по Соглашению о Торговых Аспектах Прав Интеллектуальной Собственности и по Договору об Авторском Праве Всемирной Организации Интеллектуальной Собственности (ВОИС), когда такие действия совершаются умышленно в коммерческом масштабе и с помощью компьютерной системы, за исключением любых моральных прав, предоставляемых этими Конвенциями.*
>
> *2) Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовных преступлений согласно внутригосударственному праву нарушения прав, связанных с авторским правом, как оно определено законодательством этой Стороны во исполнение обязательств, взятых ею на себя согласно Международной конвенции об охране интересов артистов-исполнителей, производителей фонограмм и вещательных организаций (Римская конвенция), Соглашению о торговых аспектах прав интеллектуальной собственности и Договору ВОИС об исполнителях и фонограммах, когда такие акты совершены умышленно, в коммерческом масштабе и с помощью компьютерной системы, за исключением любых моральных прав.*
>
> *3) Любая Сторона может сохранить за собой права в некоторых обстоятельствах не привлекать виновных к уголовной ответственности согласно положениям параграфов 1 и 2 настоящей статьи при условии, что имеются другие эффективные средства правовой защиты и что такая оговорка не ведет к частичной отмене Стороной своих международных обязательств, предусмотренных международными документами, упомянутыми в параграфах 1 и 2 настоящей статьи.*

В большинстве стран нарушение авторских прав уже квалифицируется в качестве преступления[1295] и рассмотрено в ряде международных договоров[1296]. Конвенция призвана обеспечить основополагающие

[1291] For more information on the effects of the digitalisation for the entertainment industry see above: Chapter 2.6.a.

[1292] The technology that is used is called Digital Rights Management – DRM. The term Digital rights management (DRM) is used to describe several technologies used to enforce pre-defined policies controlling access to software, music, movies, or other digital data. One of the key functions is the copy protection that aims to control or restrict the use and access to digital media content on electronic devices with such technologies installed. For further information, see: *Cunard/Hill/Barlas*, "Current developments in the field of digital rights management", available at: http://www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

[1293] Regarding the technical approach of copyright protection see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: http://www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

[1294] For details see above: Chapter 2.6.1.

[1295] Examples are 17 U.S.C. § 506 and 18 U.S.C. § 2319:

> *Section 506. Criminal offenses*
> *(a) Criminal Infringement. –- Any person who infringes a copyright willfully either –*
> *(1) for purposes of commercial advantage or private financial gain, or*
> *(2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000,*
> *shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.*
> *[...]*

принципы, касающиеся уголовной ответственности за нарушения авторских прав в целях гармонизации существующего национального законодательства. Нарушения патента или торговой марки не подпадает под это положение[1297].

Ссылка на международные соглашения

В отличие от других правовых рамок, Конвенция прямо не называет деяния преступлениями, а отсылает к ряду международных соглашений[1298]. Это один из аспектов Статьи 10, подвергаемый критике. В отличие от того, что это затрудняет определение рамок судебного преследования и что такие соглашения могут быть впоследствии изменены, возникает вопрос, должны ли страны, подписавшие Конвенцию, подписывать международные соглашения, упомянутые в Статье 10. Составители Конвенции подчеркнули, что Конвенция о киберпреступности не вводит таких обязательств[1299]. Те государства, которые не подписали упомянутые

Section 2319. Criminal infringement of a copyright
(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.
(b) Any person who commits an offense under section 506(a)(1) oftitle 17 –
(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;
(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.
(c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code –
(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;
(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and
(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.
(d)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.
(2) Persons permitted to submit victim impact statements shall include -
(A) producers and sellers of legitimate works affected by conduct involved in the offense;
(B) holders of intellectual property rights in such works; and
(C) the legal representatives of such producers, sellers, and holders.
(e) As used in this section -
(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and
(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17.

Regarding the development of legislation in the United States see: *Rayburn*, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: http://www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

[1296] Regarding the international instruments see: *Sonoda*, Historical Overview of Formation of International Copyright Agreements in the Process of Development of International Copyright Law from the 1830s to 1960s, 2006, available at: http://www.iip.or.jp/e/summary/pdf/detail2006/e18_22.pdf; *Okediji*, The International Copyright System: Limitations, Exceptions and Public Interest Considerations for Developing Countries, 2006, available at: http://www.unctad.org/en/docs/iteipc200610_en.pdf; Regarding international approaches of anti-circumvention laws see: *Brown*, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: http://www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

[1297] Explanatory Report to the Council of Europe Convention on Cybercrime No. 109.

[1298] Explanatory Report to the Council of Europe Convention on Cybercrime No. 110: "With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation (WIPO) Copyright Treaty. With regard to paragraph 2, the international instruments cited are the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

[1299] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 111 "The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

международные соглашения, тем не менее не обязаны подписывать соглашения и не принуждаются преследовать в судебном порядке деяния, которые связаны с не подписанными ими соглашениями. Статья 10 обязательна только для тех сторон, которые подписали одно из упомянутых соглашений.

Субъективная сторона

В силу своего общего характера Конвенция ограничивает судебное преследование тех деяний, которые были совершены с помощью компьютерной системы[1300]. В дополнение к деяниям, совершенным с помощью компьютерной системы, уголовная ответственность ограничивается актами, которые совершаются умышленно и в коммерческих масштабах. Термин "сознательно" соответствует термину "умышленно", который используется в других материально-правовых положениях Конвенции и учитывается в терминологии, использующейся в Статье 61 Соглашения TRIPS[1301], которое регулирует обязательства по судебному преследованию нарушений авторских прав[1302].

Промышленные масштабы

Ограничение действий в промышленных масштабах, кроме того, учитывается Соглашением по торговым аспектам прав интеллектуальной собственности (TRIPS), которое требует уголовного наказания только за "пиратство в промышленных масштабах". Поскольку большинство нарушений в системах обмена файлами совершается не в промышленных масштабах, они не подпадают под Статью 10. Конвенция направлена на определение минимальных критериев преступлений, связанных с интернетом. Таким образом, в судебном преследовании нарушений авторских прав стороны могут не ограничиваться рамками "промышленных масштабов[1303]".

Без права

В целом основные положения уголовного права, определенные в Конвенции о киберпреступности, требуют, чтобы деяние осуществлялось "без права"[1304]. Составители Конвенции указали, что термин "нарушение" уже подразумевает, что это деяние было совершено без разрешения[1305].

Ограничения и оговорки

Пункт 3 позволяет подписавшим сделать оговорку о том, что до тех пор, пока имеются другие эффективные средства правовой защиты и оговорки, не отступать от международных обязательств участников.

[1300] Explanatory Report to the Council of Europe Convention on Cybercrime No. 16 and 108.

[1301] *Article 61*
Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.

[1302] Explanatory Report to the Council of Europe Convention on Cybercrime No. 113.

[1303] Explanatory Report to the Council of Europe Convention on Cybercrime No. 114.

[1304] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1305] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 115. In addition the drafters pointed out: The absence of the term "without right" does not *a contrario* exclude application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

Проект Стэнфордской Конвенции

Неофициальный[1306] проект Стэнфордской Конвенции 1999 г. не содержит положения об уголовном преследовании нарушений авторских прав. Составители Конвенции указали, что включение нарушений авторских прав было затруднительно[1307]. Вместо этого они отсылают непосредственно к пункту существующих международных соглашений[1308].

6.2 Процессуальное право

6.2.1 Введение

Как объяснено в разделах выше, борьба с киберпреступностью требует адекватного касающегося существа уголовного права[1309]. По крайней мере, в странах гражданского права органы охраны правопорядка не будут иметь возможность расследовать преступления без ввода этих законов в действие. Но требование органов охраны правопорядка в борьбе с киберпреступностью не ограничены основными положениями уголовного законодательства[1310]. Для проведения расследований они должны обеспечить, в дополнение к профессиональной подготовке и оборудованию, процессуальные документы, которые позволят им принять меры, необходимые для выявления правонарушителя и сбора доказательств, необходимых для уголовного судопроизводства[1311]. Эти меры могут быть схожи с теми, которые предпринимаются в других расследованиях, не связанных с киберпреступностью, но в связи с тем, что преступник не обязательно должен присутствовать на или даже рядом с местом преступления, весьма вероятно, что необходимость расследования киберпреступлений будет осуществляться по-другому по сравнению с традиционными расследованиями[1312].

Причиной необходимости применения различных методов расследования является не только независимость от места действия и места преступления. В большинстве случаев для органов охраны правопорядка это с сочетанием ряда вышеуказанных проблем, проводящих уникальные расследования киберпреступлений[1313]. Если правонарушитель находится в другой стране [1314], использующей услуги, позволяющие анонимную связь, и, кроме того, совершает преступления с использованием различных терминалов доступа в интернет общего пользования, преступление трудно расследовать на основе традиционных инструментов, например, только поиск и захват. Во избежание недоразумений важно отметить, что расследования киберпреступлений

[1306] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1307] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1308] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1309] See above: Chapter 4.4.1 and Chapter 6.1.

[1310] This was as well highlighted by the drafters of the Council of Europe Convention on Cybercrime that contains a set of essential investigation instruments. The drafters of the report point out: “Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques“ see: Explanatory Report to the Council of Europe Convention on Cybercrime No. 132. Regarding the substantive criminal law provisions related to Cybercrime see above: Chapter 6.1.

[1311] Regarding the elements of a Anti-Cybercrime strategy see above: xxx. Regarding user-based approaches in the fight against Cybercrime see: *Görling*, The Myth Of User Education, 2006 at http://www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See as well the comment made by *Jean-Pieree Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: “More broadly, we have to educate users. They must all understand what they can and can’t do on the Internet and be warned of the potential dangers. As use of the Internet grows, we’ll naturally have to step up our efforts in this respect.”

[1312] Due to the protocols used in Internet communication and the worldwide accessibility there is very little need for a physical presence at the place where a service is physically offered. Due to this independence of place of action and the crime site, many criminal offences related to the Internet are transnational crimes. Regarding the independence of place of action and the result of the offence see above: Chapter 3.2.7.

[1313] Regarding the challenges of fighting Cybercrime see above: Chapter 3.2.

[1314] The pure fact that the offender is acting from a different country can go along with additional challenges for the law enforcement agencies as the investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases the investigation never the less requires an international cooperation of the authorities in both countries that in general is more time consuming compared to investigations concentrating on a single country.

требует классической детективной деятельности, а также применение традиционных инструментов расследования, но расследования киберпреступлений проходят наравне с проблемами, которые не могут быть решены только с помощью традиционных инструментов расследования[1315].

Некоторые страны уже разработали новые инструменты, позволяющие органам охраны правопорядка расследования киберпреступлений, а также традиционных преступлений, требующих анализа компьютерных данных[1316]. В отношении существенного уголовного права Конвенция о киберпреступности Совета Европы содержит ряд положений, отражающий ширину принятых минимальных стандартов, касающихся процедурных документов, необходимых для расследования киберпреступлений[1317]. Нижеследующий обзор будет ссылаться на документы, предложенные этой международной конвенцией, и, кроме того, отметит национальные подходы, выходящие за рамки положений этой Конвенции.

6.2.2 Расследования в области компьютеров и интернета (Судебная экспертиза с использованием компьютерной техники)

Существуют различные определения "судебной экспертизы с использованием компьютерной техники"[1318]. Она может быть определена как "исследование ИТ-оборудования и систем с целью получения информации для уголовного или гражданского расследования"[1319]. При совершении преступлений преступники оставляют следы[1320]. Это утверждение действует как в традиционных расследованиях, так и в компьютерных. Главным отличием традиционных расследований от расследований киберпреступлений является тот факт, что для расследования киберпреступлений, как правило, необходимы специальные методы расследования, связанные с данными, и оно может быть упрощено за счет применения специализированных программных средств[1321]. В дополнение к адекватным процедурным инструментам проведение такого анализа требуется от уполномоченных органов способности управлять и анализировать соответствующие данные. В зависимости от преступления, а также от применяемой компьютерной технологии, требования к процедурным инструментам расследования и техники проведения судебной экспертизы отличаются[1322] и становятся в один ряд с уникальными проблемами[1323].

[1315] See in this context as well: Explanatory Report to the Council of Europe Convention on Cybercrime No. 134.

[1316] For an overview about the current status of the implementation of the Convention on Cybercrime and its procedural law provisions in selected countries see the country profiles made available on the Council of Europe website: http://www.coe.int/cybercrime/.

[1317] See Art. 15 – 21 Council of Europe Convention on Cybercrime.

[1318] *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf; Regarding the need for standardisation see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2;

[1319] *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.

[1320] For an overview on different kind of evidence that can be collected by computer forensic experts see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[1321] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.

[1322] For an overview about different forensic investigation techniques related to the most common technologies see: *Carney/Rogers*, The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Vol. 2, Issue 4; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: http://www.cert.org/archive/pdf/FRGCF_v1.3.pdf.; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf ; *Urnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, Vol. 5, Issue 1; *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2; *Gupta/Mazumdar*; Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4; Hidden Disk Areas: HPA and DCO, International Journal of Digital Evidence, Vol. 5, Issue 1; *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233; *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf;

[1323] *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

В общем два эти аспекта расследования киберпреступлений тесно взаимосвязаны и часто описываются общим термином "судебная экспертиза с использованием компьютерной техники", или сбор и анализ доказательств[1324]. Как описано выше, судебная экспертиза с использованием компьютерной техники описывает применение компьютерных расследований и методов анализа для определения потенциальных доказательств. Она включает в себя широкий спектр видов анализа, начиная от общего анализа, например поиск детской порнографии на жестких дисках компьютеров[1325], до конкретных расследований, таких как судебная экспертиза iPod[1326] и получение доступа к зашифрованным файлам[1327]. Эксперты по судебной экспертизе с использованием компьютерной техники поддерживают расследования, проводимые уполномоченными полицейскими и прокурорами. В интернет расследованиях эксперты по судебной экспертизе с использованием компьютерной техники, например, могут оказать помощь в случаях [1328]:

- определение возможных цифровых следов, в частности, возможное местонахождение данных о трафике[1329];
- поддержка поставщиков услуг интернета в выявлении информации, которую они могут предоставить для поддержки расследований;
- защита собранных соответствующих данных и обеспечение целостности цепи[1330].

После того, как потенциальные доказательства выявлены, эксперты могут, к примеру, оказать помощь в:

- защите объекта компьютерной системы в ходе анализа с точки зрения возможного изменения или повреждения данных[1331];
- открытии всех соответствующих файлов на объекте компьютерной системы и носителе данных[1332];
- расшифровке зашифрованных файлов[1333];
- восстановлении удаленных файлов;
- выявлении использования компьютерных систем в случаях, когда более одного человека имело доступ к машине или устройству[1334];
- выявлении содержания временных файлов, используемых приложениями и операционной системой;
- анализе собранных доказательств[1335];
- документировании результатов анализа[1336];

[1324] See in this context ABA International Guide to Combating Cybercrime, 128 et seq.
[1325] Regarding hash-value based searches for illegal content see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 546 et seq.
[1326] *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2
[1327] *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf;
[1328] Regarding the models of Forensic Investigations see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.
[1329] *Gercke*, Cybercrime Training for Judges, 2009, page 56, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.
[1330] This process is from great importance because without ensuring the integrity of the relevant evidence the information might not be useful within criminal proceedings. For more information see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.
[1331] This process is from great importance because without ensuring the integrity of the relevant evidence the information might not be useful within criminal proceedings. For more information see: *Ciardhuain,* An Extended Model of Cybercrime Investigations, International Journal of Digital Evidence, Vol. 3, Issue 1.
[1332] This includes stored files as well as deleted files that have not yet been completely removed from the hard disk. In addition experts might be able to identify temporary, hidden or encrypted files. *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.
[1333] Regarding legal approaches related to the use of encryption technology see below: Chapter 6.2.9.
[1334] *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1.
[1335] *Gercke*, Cybercrime Training for Judges, 2009, page 55, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.
[1336] Regarding the chain of custody in cybercrime investigations see: *Nagaraja*, Investigator's Chain of Costody in Digital Evidence Recovery, available at:

- предоставлении данных для дальнейшего расследования;
- предоставлении экспертных консультаций и свидетельских показаний.

Особое участие судебных экспертов в области защиты целостности доказательств свидетельствует о том, что работа судебных экспертов сочетает в себе технические и правовые аспекты. Одна из главных задач в этом контексте является целостность цепи, что требует точного аудита исходных данных проводимого в рамках жестких требований, связанные с практической работой судебных экспертов[1337].

Масштабы возможного участия экспертов судебной экспертизы с использованием компьютерной техники демонстрируют их важность в процессе расследования. Кроме того, зависимость успеха расследования в сети интернет от наличия судебных ресурсов свидетельствует о необходимости подготовки кадров в этой области. Только в случае, если следователи либо имеют подготовку по судебной экспертизе с использованием компьютерной техники или имеют доступ к экспертам в области, возможно эффективное расследование и может быть проведено уголовное преследование киберпреступления.

6.2.3 Гарантии

В течение последних нескольких лет органами охраны правопорядка во всем мире была подчеркнута крайняя необходимость наличия инструментов для проведения адекватного расследования[1338]. Принимая это во внимание, возможно неожиданностью стало то, что Конвенция о киберпреступности была подвергнута критике в связи с процессуальными документами[1339]. Критика в основном основана на тех аспектах, что Конвенция содержит целый ряд положений, которые определяют следственные инструменты (Статьи с 16 по 21), но только в одном положении (Статья 15) речь идет о гарантиях[1340]. Кроме того, можно отметить, что в отличие от материального уголовного права в положениях Конвенции очень мало возможностей для национального регулирования реализации Конвенции[1341]. Как таковая, критика сосредоточена в основном на количественных аспектах. Действительно, Конвенция придерживается концепции централизованного регулирования гарантий вместо применения их для каждого инструмента в отдельности. Но это вовсе не обязательно приводит к более слабой защите прав подозреваемых.

Конвенция о киберпреступности была с самого начала задумана как международная основа и инструмент для борьбы с киберпреступностью, который не ограничивается исключительно странами членами Совета Европы[1342]. При обсуждении необходимых процессуальных документов составители Конвенции, в написании которой приняли участие представители и из неевропейских стран, например США и Япония, поняли, что существующие национальные подходы, связанные с гарантиями, и особенно способ охраны подозреваемых в различных уголовно-правовых системах были настолько разными, что невозможно было представить одно точное решение для всех государств-членов[1343]. Поэтому составители Конвенции решили

---

http://www.bprd.gov.in/writereaddata/linkimages/Investigators%20Chain%20of%20custody%20in%20digital%20evidence%20recovery%20Dr%20M%20K%20Nagaraja313518100.pdf.

[1337] Regarding the chain of custody in cybercrime investigations see: *Nagaraja*, Investigator's Chain of Costody in Digital Evidence Recovery, available at: http://www.bprd.gov.in/writereaddata/linkimages/Investigators%20Chain%20of%20custody%20in%20digital%20evidence%20recovery%20Dr%20M%20K%20Nagaraja313518100.pdf.

[1338] See *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801 for further reference.

[1339] *Taylor*, The Council of Europe Cybercrime Convention – A civil liberties perspective, available at http://crime-research.org/library/CoE_Cybercrime.html; Cybercrime: Lizenz zum Schnueffeln Finacial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at http://www.ccc.de.

[1340] See *Breyer,* Council of Europe Convention on Cybercrime, DUD, 2001, 595 et seqq.

[1341] Regarding the possibilities of making reservations see Article 42 of the Convention on Cybercrime:
Article 42
By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

[1342] See above: Chapter 5.1.4.

[1343] "Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The

не включать в текст Конвенции конкретные регуляторные положения, а вместо этого предложить государствам-членам обеспечить применение твердых гарантий применения национальных и международных стандартов[1344].

> ***Статья 15 – Условия и гарантии***
>
> *1 Каждая Сторона должна обеспечить установление, исполнение и применение полномочий и процедур, предусмотренных настоящим Разделом, их осуществление в соответствии с условиями и гарантиями, предусмотренными нормами ее внутригосударственного права, обеспечивающими надлежащую защиту прав человека и свобод, включая права, вытекающие из обязательств, которые Сторона взяла на себя по Европейской Конвенции о защите прав человека и основных свобод, принятой Советом Европы в 1950 году Международным пактом о гражданских и политических правах, принятым Организацией Объединенных Наций в 1966 году, а также другими применимыми международными документами по правам человека и предусматривающими принцип соразмерности.*
>
> *2 Такие условия и гарантии с учетом характера полномочий и процедур включают, среди прочего, судебный или иной независимый надзор, основания правомочности применения, ограничение сферы и сроков действия таких полномочий или процедур.*
>
> *3 В той мере, в какой это соответствует общественным интересам, в частности, надлежащему отправлению правосудия, каждая Сторона должна учитывать влияние предусмотренных данным разделом полномочий и процедур на права, ответственность и законные интересы третьих сторон.*

Статья 15 основана на том принципе, что подписавшие государства применяют условия и гарантии, которые уже существуют в соответствии со своим внутренним законодательством. Если закон обеспечивает централизованные стандарты, применимые ко всем документам следствия, эти принципы должны с таким же успехом применяться к документам относительно интернета[1345]. В случае, если внутреннее законодательство не основано на централизованном регулировании гарантий и условий, необходимо проанализировать гарантии и условия, осуществляемые в связи с традиционными документами, сопоставимыми с документами относительно интернета.

Однако Конвенция ссылается не только на гарантии, существующие в национальном законодательстве. Это может оказаться помехой тому, что требования о применении будут отличаться таким образом, что позитивные аспекты гармонизации более не будут применяться. Для тех подписавших государств, которые имеют иные правовые традиции и гарантии в реализации основных стандартов[1346], Конвенция о киберпреступности определяет минимальные стандарты, ссылаясь на фундаментальные основы, такие как нижеследующие:

- Европейская Конвенция о защите прав человека и основных свобод, принятая Советом Европы в 1950 году;
- Международный пакт о гражданских и политических правах, принятый Организацией Объединенных Наций в 1966 году;
- Другие применимые международные документы по правам человека.

Поскольку Конвенция может быть подписана и ратифицирована также странами, которые не являются членами Совета Европы[1347], важно подчеркнуть, что не только Международный пакт о гражданских и

---

modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure." See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 145.

[1344] "There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments. " See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 145.

[1345] For the transformation of safeguards to Internet-related investigation techniques see: *Taylor*, The Scope of Government Access to Copies of Electronic Communication Stored with Internet Service Providers: A Review of Legal Standards, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/taylor.pdf.

[1346] This is especially relevant with regard to the protection of the suspect of an investigation.

[1347] See: Article 37 – Accession to the Convention
1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the

политических правах ООН, а также Конвенции Совета Европы о защите прав человека и основных свобод будут приняты во внимание при оценке системы гарантий в подписавших ее государствах, не являющихся членами Конвенции о киберпреступности.

В отношении расследований киберпреступлений одной из наиболее важных положений Статьи 15 Конвенции о киберпреступности является ссылка на пункт 2 Статьи 8 Европейской конвенции по правам человека.

> ***Статья 8***
>
> *1 Каждый имеет право на уважение его личной и семейной жизни, его жилища и его корреспонденции.*
>
> *2 Не допускается вмешательство со стороны властей в осуществление этого права, за исключением случаев, когда такое вмешательство предусмотрено законом и необходимо в демократическом обществе в интересах национальной безопасности и общественного порядка, экономического благосостояния страны, в целях предотвращения беспорядков или преступлений, для охраны здоровья или нравственности или защиты прав и свобод других лиц.*

Европейский суд по правам человека предпринял усилия для более точного определения стандартов, регулирующих электронные расследования и особенно наблюдение. Сегодня прецедентное право стало одним из наиболее важных источников для международных стандартов, касающихся относящихся к связи расследований[1348]. Прецедентное право принимает во внимание серьезность вмешательства в расследования[1349], его цели[1350] и его соразмерность[1351]. Основополагающими принципами, которые могут быть извлечены из прецедентного права, являются:

- эффективная правовая основа для необходимых следственных инструментов[1352];
- правовая основа должно быть однозначной относительно данного вопроса[1353];
- юрисдикция органов охраны правопорядка должна быть предсказуемой[1354];
- надзор за связью может быть оправдан только в контексте серьезных преступлений[1355].

Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

[1348] ABA International Guide to Combating Cybercrime, page 139.

[1349] "interception of telephone conversations represent[s] a serious interference with private life and correspondence and must accordingly be based upon a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" – Case of Kruslin v. France, Application no. 11801/85.

[1350] "the requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly", Case of Malone v. United Kingdom, Application no. 8691/79

[1351] "Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application no. 5029/71.

[1352] "The expression "in accordance with the law", within the meaning of Article 8 § 2 (art. 8-2), requires firstly that the impugned measure should have some basis in domestic law", Case of Kruslin v. France, Application no. 11801/85.

[1353] "Furthermore, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject", Case of Doerga v. The Netherlands, Application no. 50210/99.

[1354] "it also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law", Case of Kruslin v. France, Application no. 11801/85.

"Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence.", Case of Malone v. United Kingdom, Application no. 8691/79

[1355] "The cardinal issue arising under Article 8 (art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application no. 5029/71.

В дополнение к этому Статья 15 Конвенции о киберпреступности принимает во внимание принцип соразмерности[1356]. Это положение особенно актуально для подписавших его государств, которые не являются членами Совета Европы. В тех случаях, когда существующая национальная система гарантий не обеспечивает надлежащей защиты подозреваемого, обязательно чтобы государства-члены разработали необходимые гарантии в процессе ратификации и осуществления.

В заключении Статьи 15 подпункт 2 Конвенции о киберпреступности относит непосредственно к некоторым из наиболее важных гарантий[1357], в том числе:

- наблюдение;
- основания, оправдывающее применение;
- ограничение процедуры с учетом масштабов и продолжительности.

В отличие от основных принципов, изложенных выше, гарантии, упомянутые здесь, нет необходимости осуществлять в отношении любого инструмента, только в случае необходимости с точки зрения характера или процедуры. Решение об этом остается на усмотрение национальных законодательных органов[1358].

Одним из важных аспектов, связанных с системой гарантий, предусмотренных в рамках Конвенции о киберпреступности, является тот факт, что способность органов охраны правопорядка гибко использовать инструменты, с одной стороны, и обеспечивать эффективные гарантии, с другой стороны, зависит от создания градационной системы гарантий. Конвенция прямо не препятствует сторонам в осуществлении той же гарантии, например, требование о наличии судебного решения, для всех инструментов, но такой подход позволил бы влиять на гибкость органов охраны правопорядка. Способность обеспечить надлежащую защиту подозреваемого человека в градационной системе гарантий во многом зависит от баланса между потенциальным воздействием расследование инструмента с соответствующими гарантиями. Для достижения этой цели необходимо проводить различие между менее и более интенсивными инструментами. Есть ряд примеров такой дифференциации в Конвенции о киберпреступности, которые позволяют сторонам дальнейшее развитие системы градационной гарантий. Они включают в себя:

- Разграничение между перехватом данных о содержании (Статья 21)[1359] и сбором данных о трафике (Статья 20)[1360]. В отличие от сбора данных о трафике перехват данных о содержании причисляется к тяжким преступлениям[1361].
- Разграничение между оперативным обеспечением сохранности хранимой компьютерной информации (Статья 16)[1362] и представлении хранимых компьютерных данных, основанных на порядке производства (Статья 18)[1363]. Статья 16 предоставляет органам охраны правопорядка только порядок сохранения данных, но не их раскрытие[1364].

[1356] "Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures." See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 146.

[1357] The list is not concluding. See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 146.

[1358] "National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards." See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 147.

[1359] See below 6.2.9

[1360] See below 6.2.10.

[1361] "Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle." See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 146.
"Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 230.

[1362] See below 6.2.4.

[1363] See below 6.2.7.

[1364] As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorise the law enforcement agencies to prevent the deletion of the relevant data. The advantage of a separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for their application.

- Разграничение между обязанностью представить "информацию пользователя"[1365] и "компьютерные данные"[1366] в Статье 18[1367].

Если интенсивность инструмента расследования и потенциальное воздействие на подозреваемого оценены правильно и гарантии сформулированы в соответствии с результатами проведенного анализа, система градационных гарантий не приводит к несбалансированной системе процессуальных инструментов.

6.2.4 Ускоренное сохранение и раскрытие сохраненной компьютерной информации (Быстрая заморозка)

Идентификация преступника, совершившего киберпреступление, часто требует анализа данных о трафике[1368]. В частности, IP-адреса, используемые преступником, могут помочь органам охраны правопорядка отследить его. Если правоохранительные органы имеют доступ к соответствующим данным трафика, в некоторых случаях можно определить преступника, даже использующего терминал доступа в интернет общего пользования, не требующий идентификации[1369].

Одной из основных трудностей, с которыми сталкиваются следователи, является тот факт, что данные о трафике тесно связаны с информационными сведениями, которых нередко автоматически удаляются через довольно короткое время. Причина данного автоматического удаления состоит в том, что после окончания процесса, например, отправки электронной почты, доступа в интернет или скачивание фильма, данные о трафике, сформированные в ходе процесса и обеспечения того, чтобы этот процесс мог быть осуществлен, более не требуются. Что касается экономических аспектов этой деятельности, то большинство поставщиков услуг интернета заинтересованы в как можно более быстром удалении информации, так как хранить данные в течение более длительных периодов потребуется большая по размеру (более дорогая) емкость памяти[1370].

Однако экономические аспекты не являются единственной причиной, почему правоохранительные органы должны проводить свои расследования быстро. Некоторые страны имеют строгие законы, которые запрещают хранение определенных данных о трафике по окончании процесса. Одним из примеров таких ограничений является Статья 6 Директивы Европейского Союза о частной жизни и электронной связи[1371].

> ***Статья 6 – Данные о трафике***
>
> *1 Данные о трафике, относящиеся к абонентам и пользователям, обрабатываемые и сохраняемые поставщиком услуг сети связи общего пользования или услуг электронной связи общего пользования, должны быть удалены или сделаны анонимными, когда более нет необходимости передачи сообщения без ущерба для пунктов 2, 3 и 5 настоящей статьи и Статьи 15 (1).*
>
> *2 Данные о трафике, необходимые для целей биллинга и взаимосвязанных платежей, могут быть обработаны. Такая обработка допускается только до конца периода, в течение которого этот платеж может быть оспорен на законных основаниях или взыскан в суде.*

Время является важным аспектом интернет расследований. В общем, поскольку вполне вероятно, что какое-то время пройдет между совершением деяния, обнаружением преступления, а также уведомлением органов

[1365] A definition of the term “subscriber information” is provided in Art. 18 Subparagraph 3 Convention on Cybercrime.
[1366] A definition of the term “computer data” is provided in Art. 1 Convention on Cybercrime.
[1367] As described more in detail below the differentiation between “computer data” and “subscriber information” the Art. 18 Convention on Cybercrime enables the signatory states to develop graded safeguards with regard to the production order.
[1368] “Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required”,See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 155.; Regarding the identification of suspects by IP-based investigations see: *Gercke*, Preservation of User Data, DUD 2002, 577 et seq.
[1369] *Gercke*, Preservation of User Data, DUD 2002, 578.
[1370] The cost issue was especially raised within the discussion about data retention legislation in the EU. See for example: E-communications service providers remain seriously concerned with the agreement reached by European Union Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005, available at: http://www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.
[1371] Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

охраны правопорядка, важно создать механизмы, которые предохраняют соответствующие данные от удаления иногда в течение длительного процесса расследования. В связи с этим, в настоящее время обсуждается два различных подхода[1372]:

- сохранение данных; и,
- обеспечение сохранности данных ("Быстрая заморозка").

Обязательства сохранения данных обязательств вынуждают поставщика услуг интернета сохранить данные о трафике в течение определенного периода времени[1373]. В соответствии с последними законодательными подходами отчеты должны храниться в течение периода от 6 до 24 месяцев[1374]. Это должно позволить органам охраны правопорядка получать доступ к данным, которые необходимы для выявления преступника даже спустя месяцы после совершения правонарушения[1375]. Обязательства хранения данных недавно приняты парламентом Европейского союза[1376], и в настоящее время также обсуждаются в США[1377]. Относительно принципов хранения данных с дополнительной информацией можно ознакомиться ниже.

Конвенция о киберпреступности

Сохранность данных является другим подходом к обеспечению того, чтобы расследование киберпреступлений не провалилось только потому, что данные о трафике были удалены в ходе длительного расследования[1378]. В соответствии с законами о хранении данных, органы охраны правопорядка могут обязать поставщика услуг об удалении определенных данных. Ускоренное сохранение компьютерных данных является одним из инструментов, который должен дать органам охраны правопорядка возможность реагировать незамедлительно и избегать риска удаления данных в результате длительного расследования[1379]. Составители Конвенции о киберпреступности решили сосредоточить внимание на "ускоренном сохранении данных" вместо "сохранение данных[1380]". Регулирование может быть найдено в Статье 16 Конвенции о киберпреступности.

[1372] The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantaged and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data retention obligation. “Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible.” Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001. A similar discussion took place during the negotiation of the Convention on Cybercrime. The drafters explicitly pointed out, that the Convention does not establish a data retention obligation. See Explanatory Report to the Convention on Cybercrime, No. 151., available at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

[1373] Regarding The Data Retention Directive in the European Union, see *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1, available at: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J.__Int'l_L._233_(2007).pdf; *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et seq.

[1374] Art. 6 Periods of Retention
Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.
Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[1375] See: Preface 11. of the European Union Data Retention Directive: “Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive.”

[1376] Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

[1377] See for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes - Internet StoppingAdults Facilitating the Exploitation of Today’s Youth Act (SAFETY) of 2007, available at: http://www.govtrack.us/congress/bill.xpd?bill=h110-837. Regarding the current situation in the US see: ABA International Guide to Combating Cybercrime, page 59.

[1378] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

[1379] However, it is recommended that States consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases. Explanatory Report to the Convention on Cybercrime, No. 160.

[1380] *Gercke*, Cybercrime Training for Judges, 2009, page 63, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

Статья 16 – Оперативное обеспечение сохранности хранимой компьютерной информации

1 Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы ее компетентные органы путем выпуска распоряжений или аналогичным образом оперативно обеспечивали сохранность конкретных компьютерных данных, включая данные о трафике, которые хранятся средствами компьютерной системы, в частности, когда имеются основания полагать, что эти компьютерные данные особенно подвержены риску утраты или изменения.

2 Если Сторона реализует положения приведенного выше параграфа 1 посредством выпуска распоряжения какому-либо лицу об обеспечении сохранности конкретных хранимых компьютерных данных, находящихся во владении или под контролем этого лица, то эта Сторона принимает такие законодательные и иные меры, какие могут потребоваться, для того чтобы обязать данное лицо хранить эти компьютерные данные и обеспечивать их целостность в течение необходимого периода времени, не превышающего девяноста дней, с тем чтобы компетентные органы могли добиться раскрытия этих компьютерных данных. Сторона может предусмотреть возможность последующего продления действия такого распоряжения.

3 Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы обязать хранителя или другое лицо, которому поручено обеспечивать сохранность компьютерных данных, сохранять конфиденциальность выполнения таких процедур в течение срока, предусмотренного ее внутригосударственным правом.

4 Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями Статей 14 и 15.

С точки зрения поставщика услуг интернета ускоренное сохранение данных является менее интенсивным инструментом по сравнению с сохранением данных[1381]. Поставщикам услуг интернета не нужно хранить все данные для всех пользователей, вместо этого они должны обеспечить неудаление конкретных данных при получении распоряжения компетентного органа. Ускоренное сохранение данных предоставляет преимущества, так как оно охватывает сохранение данных не только с точки зрения от поставщика, но и с точки зрения защиты данных. Оно не является необходимым для сохранения данных от миллионов пользователей интернета, а только данные, которые имеют отношение к возможным подозреваемым в уголовных расследованиях. Тем не менее, важно отметить, что сохранение данных предлагает преимущества в тех случаях, когда данные будут удалены сразу после окончания правонарушения. В этих случаях указание об ускоренном сохранения данных может, в отличие от обязательства сохранения данных, быть не в состоянии не допустить удаления соответствующих данных.

Указание, соответствующее Статье 16, обязывает поставщика только сохранить данные, обработанные поставщиком и не удаленные во время получения указания поставщиком[1382]. Это не только данные о трафике, данные о трафике поминается просто как один из примеров. Статья 16 не заставляет поставщика начать сбор информации, которую они, как правило, не сохраняют[1383]. Кроме того, Статья 16 не обязывает поставщика передавать соответствующие данные компетентным органам. Это положение разрешает органам охраны правопорядка только предупреждение удаления соответствующих данных, но не обязывает поставщиков передавать данные. Обязательство передачи регулируется Статьями 17 и 18 Конвенции о киберпреступности. Преимуществом разделения обязательства хранения данных и обязательства раскрывать их является возможность требовать различные условия их применения[1384]. Что касается важности немедленного реагирования, было бы полезно, например, отменить требование судебного предписания и разрешить исполнительное предписание или указание полиции о сохранении данных[1385]. Это позволило бы компетентным органам реагировать быстрее. Защита прав подозреваемого может быть достигнута требованием наличия предписания на раскрытие информации[1386].

[1381] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 803.

[1382] 'Preservation' requires that data, which already exists in a stored form, be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

[1383] Explanatory Report No 152.

[1384] Regarding the advantages of a system of graded safeguards see above: Chapter 6.2.3.

[1385] "The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor)". See Explanatory Report to the Convention on Cybercrime, No. 160.

[1386] The drafters of the Convention on Cybercrime tried to approach the problems related to the need of immediate action from law enforcement agencies on the one hand side and the importance of ensuring safeguards on the other hand side in a number of ways. Another example for the approach is related to the production order (Art. 18). The drafters suggested that the requirements for the

Раскрытие сохраненных данных помимо других аспектов регулируется Статьей 18 Конвенции о киберпреступности:

> ***Статья 18 – Порядок производства***
>
> *1 Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы предоставить ее компетентным органам полномочия отдавать распоряжения:*
>
> *a) лицу на ее территории о предъявлении конкретных компьютерных данных, находящихся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на носителе компьютерных данных; и*
>
> *b) поставщику услуг, предлагающему свои услуги на ее территории, о предъявлении находящейся во владении или под контролем этого поставщика услуг информации о его абонентах.*
>
> *2 Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями Статей 14 и 15.*
>
> *3 Для целей настоящей статьи термин "информация об абонентах" означает любую имеющуюся у поставщика услуг информацию о его абонентах в форме компьютерных данных или любой другой форме, кроме данных о трафике или содержания, с помощью которой можно установить:*
>
> *a) вид используемой услуги связи, принятые с этой целью меры технического обеспечения и период оказания услуги;*
>
> *b) идентичность абонента, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание;*
>
> *c) любые другие сведения о месте установки коммуникационного оборудования, доступные согласно соглашению или договору на обслуживание.*

На основании Статьи 18 подраздел 1 a) Конвенции о киберпреступности, поставщики, осуществившие сохранение данных, могут быть обязаны их раскрыть.

Статья 18 Конвенции о киберпреступности применима не только после того, как получено предписание о сохранении в соответствии со Статьей 16 Конвенции о киберпреступности[1387]. Это положение является общим инструментом, который может использоваться органами охраны правопорядка. Если получатель судебного приказа о предоставлении информации добровольно передает запрашиваемые данные, то действия органов охраны правопорядка сводятся к извлечению аппаратных средств, а они могут применять менее строгий судебный приказ. По сравнению с фактическим извлечением аппаратных средств, порядок предоставления соответствующей информации в целом является менее строгим. Его применение особенно актуально в тех случаях, когда судебное расследование не требует доступа к аппаратным средствам.

В дополнение к обязательству представить компьютерные данные, Статья 18 Конвенции о киберпреступности определяет порядок представления информации об абонентах органам охранам правопорядка. Этот инструмент имеет большое значение в расследованиях на основе IP. Если правоохранительные органы смогут определить IP-адрес, использованный правонарушителем при совершении преступления, они должны будут определить лицо[1388], использовавшее IP-адрес на момент

---

handout of data to law enforcement agencies could be adjusted in relation to the categories of data. See Explanatory Report to the Convention on Cybercrime No. 174: „The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

[1387] *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1388] An IP-address does not necessary immediately identify the offender. If law enforcement agencies know the IP-address an offender used to commit an offence this information does only enable them to identify the connection used to log on to the Internet. If a group of people had access to this

совершения преступления. На основании подраздела 1 б) Статьи 18 Конвенции о киберпреступности, поставщик обязан представить абонентом информацию об абонентах, перечисленную в подразделе 3 Статьи 18[1389].

В тех случаях, когда органы охраны правопорядка отслеживают маршрут к правонарушителю и нуждаются в немедленном доступе для идентификации пути, по которому была осуществлена передача сообщения. Статья 17 позволяет им затребовать ускоренное частичное раскрытие данных о трафике.

> ***Статья 17 – Оперативное обеспечение сохранности и частичное раскрытие данных о трафике***
>
> *1 Каждая Сторона должна принимать в отношении данных о трафике, сохранность которых должна быть обеспечена в соответствии со Статей 16, такие законодательные и иные меры, какие могут быть необходимы для того, чтобы:*
>
> *a) гарантировать, чтобы такое оперативное обеспечение сохранности данных о трафике было возможным независимо от того, один или более поставщиков услуг были вовлечены в передачу соответствующего сообщения; и*
>
> *b) гарантировать оперативное раскрытие компетентным органам этой Стороны или лицу, назначенному этими органами, достаточного количества данных о трафике, которое позволит соответствующей Стороне идентифицировать поставщиков услуг и путь, которым передавалось данное сообщение.*
>
> *2 Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями Статей 14 и 15.*

Как упоминалось выше, Конвенция строго разделяет обязательство сохранения данных по запросу и обязательство передавать их компетентным органам[1390]. Статья 17 предусматривает четкую классификацию, каким образом сочетать обязательства по обеспечению сохранности данных о трафике в тех случаях, когда в обязательство раскрыть необходимую информацию для определения сквозного пути до правонарушителя были вовлечены несколько поставщиков услуг. Без такого частичного раскрытия информации органы охраны правопорядка в ряде случаев не в состоянии отследить правонарушителя при наличии более одного поставщика услуг[1391]. В связи с сочетанием этих двух обязательств, различным образом затрагивающих права подозреваемых, необходимо обсудить точку зрения гарантий, относящихся к этому инструменту.

Типовой закон Содружества о компьютерах и компьютерных преступлениях

Аналогичные подходы имеются и в Типовом законе Содружества от 2002 года[1392].

Положения

> ***Раздел 15***
>
> *Если следователь установил на основе заявления офицера полиции в том, что определенные компьютерные данные, либо в распечатанном, либо ином виде представления информации, действительно необходимы в целях уголовного расследования или уголовного дела, следователь может постановить, что:*
>
> *a) лицо на территории [постановляющей страны] под контролем компьютерной системы производит из системы указанные компьютерные данные либо в виде распечатки, либо в другом понятном виде вывода данных; и*

---

connection (e.g. in an Internet café) further investigations are necessary to identify the offender.

[1389] If the offender is using services that do not require a registration or the subscriber information provided by the user are not verified Art. 18 Subparagraph 1b) will not enable the law enforcement agencies to immediately identify the offender. Art. 18 Subparagraph 1b) is therefore especially relevant with regard to commercial services (like providing Internet access, commercial e-mail or hosting services).

[1390] *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

[1391] "Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination." See Explanatory Report to the Convention on Cybercrime, No. 167.

[1392] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

b) поставщик услуг интернет в [постановляющей стране] производит информацию о лицах, которые пользуются услугами на основе подписки или иной основе; и

c)[1393] *лицо на территории [постановляющей страны], имеющее доступ к определенной компьютерной системе, обрабатывает и комплектует определенные компьютерные данные из системы и предоставляет их определенному лицу.*

Раздел 16[1394]

Если офицер полиции установил, что сохраняемые в компьютерной системе данные, действительно, необходимы в целях уголовного расследования, сотрудник полиции может, путем направления письменного уведомления лицу, под управлением которого находится компьютерная система, потребовать от этого лица достаточные данные о трафике об определенном соединении для идентификации:

a) поставщиков услуг; и

b) путь, по которому была произведена передача в соединении.

Раздел 17

1) Если офицер полиции установил, что:

a) данные, хранимые в компьютерной системе, действительно, необходимы в целях уголовного расследования; и

b) существует риск того, что данные могут быть уничтожены или стать недоступны;

офицер полиции может, путем направления письменного уведомления лицу, под управлением которого находится компьютерная система, потребовать от этого лица гарантий, что данные, определенные в уведомлении, будут сохранены в течение периода до 7 дней, как указано в уведомлении.

2) Этот период может быть продлен более 7 дней, если на основании заявления лица, не являющегося стороной в деле, но имеющего в нем интерес, [судья] [следователь] разрешает продление на дополнительный определенный период времени.

6.2.5 Сохранение данных

Обязательство сохранения данных побуждает поставщика услуг интернета сохранять данные о трафике в течение определенного периода времени[1395]. Выполнение обязательства сохранения данных является подходом с целью избежания вышеупомянутых трудностей в получении доступа к данным о трафике, прежде чем они будут удалены. Одним из примеров такого подхода является директива Европейского союза о сохранении данных[1396].

Статья 3 – Обязательство сохранения данных

1 В порядке отступления от положений Статей 5, 6 и 9 директивы 2002/58/EC, государства-члены должны принять меры для обеспечения того, чтобы данные, указанные в Статье 5 настоящей Директивы, сохранялись в соответствии с ее положениями, в той мере, в которой эти данные генерируются или обрабатывается поставщиками общедоступных услуг

[1393] Official Note: *As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.*
Official Note: *Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.*

[1394] The Commonwealth Model Law contains an alternative provision:
"Sec. 16": If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:
(a) the service providers; and
(b) the path through which the communication was transmitted.

[1395] For an introduction to data retention see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et seq; *Blanchette/Johnson*, Data retention and the panoptic society: The social benefits of forgetfulness, available at: http://polaris.gseis.ucla.edu/blanchette/papers/is.pdf.

[1396] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

электронной связи или сети связи общего пользования в рамках своей юрисдикции в процессе предоставления соответствующих услуг связи.

2 Обязательство сохранять данные, предусмотренные в пункте 1, должно включать в себя сохранение данных, определенное в Статье 5, относительно с неудачных попыток вызова, когда эти данные создаются или обрабатываются и хранятся (для данных телефонии) либо регистрируются (для данных интернет) поставщиками услуг общедоступных электронных сообщений или сети связи общего пользования в пределах юрисдикции государств-членов, заинтересованных в процессе предоставления услуг связи. Эта директива не требует сохранения данных о вызовах без установления соединения.

Статья 4 – Доступ к данным

Государства-Члены должны принять меры для обеспечения того, чтобы сохранение данные в соответствии с настоящей Директивой обеспечивалось только компетентными национальными органами в определенных случаях и в соответствии с национальным законодательством. Процедуры, которым надлежит следовать, и условия, которые должны быть выполнены для получения доступа к сохраненным данным в соответствии с необходимостью и пропорциональности требований, должны быть определены каждым государством-членом в своем национальном законодательстве с учетом соответствующих положений законодательства Европейского Союза или международного публичного права и, в частности, Европейской конвенции по правам человек в трактовке Европейского суда по правам человека.

Статья 5 – Категории данных, которые должны быть сохранены

1 Государства-Члены должны обеспечить, чтобы на основании этой директивы сохранялись следующие категории данных:

a) данные, необходимые для отслеживания и идентификации источника сообщения:

1) касающиеся фиксированной телефонной связи и мобильной телефонной связи:

i) номер телефона вызывающего;

ii) имя и адрес абонента или зарегистрированного пользователя;

2) касающиеся доступа в интернет, электронной почты интернет и Интернет-телефонии:

i) выделенный идентификатор пользователя(ей);

ii) идентификатор пользователя и телефонные номера, выделенные для любого соединения при выходе на телефонную сеть общего пользования;

iii) имя и адрес абонента или зарегистрированного пользователя, которому IP-адрес, идентификатор пользователя или номер телефона был выделен на время соединения;

b) данные, необходимые для определения назначения сообщения:

1) касающиеся фиксированной телефонной связи и мобильной телефонной связи:

i) набранный номер a) (вызываемый телефонный номер a)), и, в случаях предоставления дополнительных услуг, таких как переадресация вызовов и передача вызовов, количество и номера, по которым вызов был маршрутизирован;

ii) имя (имена) и адрес(а) абонента(ов) или зарегистрированного пользователя(ей);

2) касающиеся электронной почты интернет и Интернет-телефонии:

i) идентификатор пользователя или номер телефона получателя(ей), которому предназначен вызов Интернет-телефонии;

ii) имя (имена) и адрес(а) абонента(ов) или зарегистрированного пользователя и идентификатор пользователя получателя, которому предназначен вызов;

c) данные, необходимые для определения даты, времени и продолжительности соединения:

1) касающиеся фиксированной телефонной связи и мобильной телефонной связи, дата и время начала и окончания соединения;

2) касающиеся доступа в интернет, электронной почты интернет и Интернет-телефонии:

i) дата и время входной и выходной регистрации услуги доступа в интернет, на основе определенных временных зон, а также IP-адрес, независимо от того, динамический он или статический, выделенный поставщиком услуг доступа в интернет для соединения, а также идентификатор пользователя абонента или зарегистрированного пользователя;

ii) дата и время входной и выходной регистрации услуги электронной почты интернет или Интернет-телефонии, на основе определенных временных зон;

d) данные, необходимые для определения типа соединения:

1) касающиеся фиксированной телефонной связи и мобильной телефонной связи: используемая услуга телефонии;

2) касающиеся электронной почты интернет и Интернет-телефонии: используемая услуга интернет;

e) данные, необходимые для идентификации пользовательского оборудования связи или что оно собой представляет:

1) касающиеся фиксированной телефонной связи, номера телефонов вызывающего и вызываемого;

2) касающиеся и мобильной телефонной связи:

i) номера телефонов вызывающего и вызываемого;

ii) Уникальный международный идентификатор абонента (IMSI) вызывающей стороны;

iii) Уникальный международный идентификатор мобильного оборудования (IMEI) вызывающей стороны;

iv) IMSI вызываемой стороны;

v) IMEI вызываемой стороны;

vi) в случае анонимных услуг с предоплатой, дата и время первоначальной активации услуг и указатель местоположения (идентификатор ячейки), с которого была активирована услуга;

3) касающиеся доступа в интернет, электронной почты интернет и Интернет-телефонии:

i) номер телефона и вызываемого для доступа с помощью телефонного вызова;

ii) цифровая абонентская линия (DSL) или другая конечная точка источника составителя данного сообщения;

f) данные, необходимые для идентификации положения мобильного:

1) указатель местонахождения (идентификатор ячейки) в начале соединения;

2) данные, определяющие географическое расположения ячеек с учетом их указателей местоположения (идентификатор ячейки) в течение периода, за который сохраняются данные сообщения.

2 В соответствии с этой директивой никакие данные, раскрывающие содержание сообщения, не могут быть сохранены.

Статья 6 – Периоды сохранения

Государства-Члены должны обеспечить, чтобы категории данных, указанных в Статье 5, сохранялись в течение не менее шести месяцев и не более двух лет с даты соединения.

Статья 7 – Защита данных и безопасность данных

Без ущерба для положений, принятых в соответствии с Директивой 95/46/EC и Директивой 2002/58/EC, каждое государство-член должно обеспечить, чтобы поставщики общедоступных услуг электронной связи или сети связи общего пользования соблюдали, как минимум, следующие принципы безопасности данных в отношении данных, сохраняемых в соответствии с этой директивой:

a) сохраняемые данные должны быть того же качества и с той же защитой, как данные в сети;

b) данные должны быть при применении соответствующих технических и организационных мер защищены от случайного или незаконного уничтожения, случайной потери или изменения, или несанкционированное или незаконное хранения, обработку, доступа или раскрытия;

c) данные должны быть при применении соответствующих технических и организационных мер обеспечены тем, чтобы доступ к ним могли получить только специально уполномоченные лица, и

d) данные, за исключением тех, к которым может иметь место доступ и сохранение, должны быть уничтожены в конце этого периода сохранения.

Статья 8 – Требования к хранению сохраняемых данных

Государства-Члены должны обеспечить, чтобы данные, указанные в Статье 5, сохраняемых в соответствии с настоящей директивой таким образом, чтобы сохраняемые данные и любая другая необходимая информация, касающаяся таких данных может быть передана по запросу компетентных органов без неоправданных задержек.

Тот факт, что ключевая информация о каких-либо соединениях по сети интернет должна быть охвачена Директивой, привел к интенсивной критике со стороны организаций по защите прав человека[1397]. Это, в свою очередь, может привести к пересмотру конституционными судами самой директивы и ее реализации[1398]. Кроме того, в своем заключении по делу Productores de Música de España (Promusicae) против Telefónica de España[1399], советник Европейского суда генеральный адвокат Юлиана Кокот указала на сомнительность выполнения обязательств сохранения данных без нарушения основных прав человека[1400]. Трудности, возникающие в связи с введением таких регуляторных действий, уже указывались группой восьми в 2001 году[1401].

Но критика не ограничивается только этим аспектом. Еще одной причиной того, почему сохранение данных оказалось менее эффективным в борьбе с киберпреступностью является тот факт, что обязательства могут быть обойдены. Простейшие пути, чтобы обойти обязательства сохранения данных включают в себя:

- использование различных о терминалов доступа в интернет общего пользования или мобильных телефонов с предоплатой услуг передачи данных, которые не требуют регистрации, и[1402]

[1397] See for example: Briefing for the Members of the European Parliament on Data Retention, available at: http://www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: http://www.vibe.at/aktionen/200205/data_retention_30may2002.pdf; Regarding the concerns related to a violation of the European Convention on Human Rights see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 et seq.

[1398] See: Heise News, 13,000 determined to file suit against data retention legislation, 17.11.2007, available at: http://www.heise.de/english/newsticker/news/99161/from/rss09.

[1399] Case C-275/06.

[1400] See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court does usually but not invariably follow the advisors conclusion.

[1401] In a G8 Meeting in Tokyo experts discussed the advantaged and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

[1402] Regarding the challenges for law enforcement agencies related to the use of means of anonymous communication see above: Chapter 3.2.12.

- использование услуг анонимной связи, осуществляемых (по крайней мере, частично) в странах, с отсутствием обязательств сохранения данных[1403].

Если преступники используют различные терминалы общего пользования или мобильный телефон с предоплатой услуг передачи данных, где нет необходимости регистрации данных, сохраняемых поставщиками услуг, обязательство сохранения данных приведет органы охраны правопорядка только к поставщику услуг, а не к реальному преступнику[1404].

Преступники, кроме того, могут обойти обязательство сохранения данных с помощью серверов анонимной связи[1405]. В этом случае, органы охраны правопорядка могут доказать тот факт, что преступник и использовал серверы анонимной связи, но из-за отсутствия доступа к данным о трафике в стране, где находится сервер анонимной связи, они не смогут доказать участия преступника в совершении преступления или уголовного преступления[1406].

В связи с тем, фактически очень легко обойти положение, введение сохранение данных в законодательстве Европейского союза сочетается с опасениями, что этот процесс потребует сторонний мер, необходимых для обеспечения действенности этого документа. Возможные дополнительные меры могли бы включать в себя обязательство регистрацию до использования услуг в режиме онлайн[1407] или запрет на использование технологий анонимной связи[1408].

6.2.6 Поиск и извлечение

Хотя новые инструменты расследования, такие как сбор данных о трафике в реальном масштабе времени и использование дистанционного судебного программного обеспечения для выявления преступника, находятся в стадии обсуждения и уже введены в некоторых странах, поиск и арест остается одним из наиболее важных инструментов расследования[1409]. Как только преступник найден, и органы охраны правопорядка извлекают его ИТ-оборудование, эксперты судебной экспертизы с использованием компьютерной техники могут проанализировать оборудования для сбора доказательств, необходимых для судебного преследования[1410].

Возможность смены места или изменения процедур поиска и извлечения в настоящее время обсуждается в некоторых европейских странах и в Соединенных Штатах[1411]. Возможность избежать необходимости войти в дом подозреваемого для поиска и извлечения компьютерной техники будет представлена онлайновым поиском. Этот инструмент, который будет более подробно описан в разделах ниже, представляет процедуру,

---

[1403] Regarding the technical discussion about traceability and anonymity see: CERT Research 2006 Annual Report, page 7 et seq., available at: http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[1404] An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of the Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorisation. In addition he is obliged to request an identification of his customers prior to the use of this services. Decree-Law 27 July 2005, no. 144. - Urgent measures for combating international terrorism. For more information about the Decree-Law see for example the article Privacy and data retention policies in selected countries available at http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[1405] See: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91 – available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

[1406] Regarding the impact of use of anonymous communication technology on the work of law enforcement agencies see above: Chapter 3.2.12.

[1407] Decree-Law 27 July 2005, no. 144. - Urgent measures for combating international terrorism. For more information about the Decree-Law see for example the article Privacy and data retention policies in selected countries available at http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[1408] Regarding the protection of the use of anonymous mean of communication by the United States constitution *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 82 –available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

[1409] A detailed overview about the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 et seq. For more information on Computer-related Search and Seizure see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 et seqq.; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 et seqq. Regarding remote live search and possible difficulties with regard to the principle of "chain of custody see: *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law and Technology Vol. 9, Issue 2, 2005, available at: http://www.lawtechjournal.com/articles/2005/05_051201_Kenneally.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

[1410] Regarding the involvement of computer forensic experts in the investigations see above: Chapter 6.2.2.

[1411] Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security , available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: http://www.news.com/8301-10784_3-9769886-7.html.

при которой органы охраны правопорядка получают доступ к компьютеру подозреваемого через интернет для выполнения процедур секретного поиска[1412]. Несмотря на то, что органы охраны правопорядка могут иметь прямую выгоду от незнания подозреваемого о проведении расследования, физический доступ к аппаратным средствам дает более эффективные методы расследования[1413]. Это подчеркивает важную роль процедур поиска и извлечения в интернет-расследованиях.

Конвенция о киберпреступности

Большинство национальных уголовно-процессуальных законов содержат положения, позволяющие органам охраны правопорядка осуществлять поиск и извлечение объектов[1414]. Причиной, по которой составители Конвенции о киберпреступности, тем не менее, включают в нее положения, касающиеся поиска и извлечения, является тот факт, что национальные законы зачастую не охватывают процедуры поиска и извлечения, связанные с данными[1415]. Некоторые страны, например, ограничивают применение процедуры извлечения для извлечения физических объектов[1416]. Исходя из этих положений, следователи могут извлечь весь сервер, а не только соответствующие данные, копируя их на сервере. Это может вызвать трудности в тех случаях, когда соответствующая информация хранится на сервере вместе с данными о сотнях других пользователей, которые больше не будут доступны после извлечения сервера органами охраны правопорядка. Еще один пример, когда традиционный поиск и извлечение материальных ценностей не является достаточным, – это случай, когда органы охраны правопорядка не знают физическое расположение сервера, но они могут иметь доступ к нему через интернет[1417].

Подпункт 1 Статьи 19 Конвенции о киберпреступности призван создать инструмент, который дает возможность поиска компьютерных систем, которые являются такими же эффективными, как традиционные процедуры поиска[1418].

> ***Статья 19 – Поиск и извлечение хранимых компьютерных данных***
>
> *1 Каждая Сторона должна принимать законодательные и иные меры, которые могут потребоваться для предоставления ее компетентным органам полномочий поиска или иной аналогичный доступ к:*
>
> *a) компьютерным системам или их частям, а также хранящимся в них компьютерным данным; и*
>
> *b) носителям компьютерных данных, на которых могут храниться искомые компьютерные данные, на ее территории.*

Несмотря на то, что процедуры поиска и извлечения является инструментом, часто применяемым следователями, существует целый ряд проблем, которые сопровождают его применение в расследовании киберпреступлений[1419]. Одна из главных трудностей состоит в том, что ордера на поиск зачастую ограничиваются определенными местами, например, в доме подозреваемого[1420]. Что касается поиска

[1412] See below: Chapter 6.2.12.

[1413] Apart from the fact that direct access enables the law enforcement agencies to examine the physical condition of storage media physical access to a computer system it is the only way to ensure that the files on the suspects computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[1414] See Explanatory Report to the Convention on Cybercrime, No. 184.

[1415] "However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data." Explanatory Report to the Convention on Cybercrime, No. 184. Regarding the special demands with regard to computer related search and seizure procedures see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

[1416] Explanatory Report No. 184.

[1417] Regarding the difficulties of online-search procedures see below: Chapter 6.2.12.

[1418] "However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record." Explanatory Report to the Convention on Cybercrime, No. 187.

[1419] *Gercke*, Cybercrime Training for Judges, 2009, page 69, available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1420] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 et seq.

компьютерных данных, в ходе следствия может оказаться, что подозреваемый хранил их не на локальных жестких дисках, а на внешнем сервере, доступ к которому осуществляется через интернет[1421]. Использование интернет-серверов для хранения и обработки данных становится все более популярным среди пользователей интернета ("облачные вычисления"). Одним из преимуществ хранения информации на интернет-серверах является тот факт, что информацию можно получить из любого места, где есть подключение к интернету. Для уверенности в том, что расследование может быть проведено эффективно, важно сохранять определенную гибкость в проведении расследований. Если следователи обнаружат, что соответствующая информация хранится в другой компьютерной системе, они должны иметь возможность расширить поиск в эту систему[1422]. Конвенция о киберпреступности адресует этот вопрос в Статье 19 подпункт 2.

> ***Статья 19 – Поиск и извлечение хранимых компьютерных данных***
>
> *[…]*
>
> *2 Каждая Сторона принимает законодательные и иные меры, необходимые для обеспечения того, чтобы в случае, когда ее компетентные органы производят поиск или получают аналогичный доступ к определенной компьютерной системе или ее части в соответствии с положениями параграфа 1a) и имеют основания полагать, что искомые данные хранятся в другой компьютерной системе или ее части на территории этой Стороны, и такие данные на законном основании могут быть получены из первой системы или с ее помощью, компетентные органы имели возможность оперативно распространить поиск или иной аналогичный доступ на другую систему.*

Еще одна проблема связана с извлечением компьютерных данных. Если следователи пришли к выводу, что извлечение аппаратных средств, используемых для хранения информации, не является необходимым или будет неадекватным, им могут потребоваться другие инструменты, которые позволили бы им продолжать процедуры поиска и извлечение соответствующих хранимых компьютерных данных[1423]. Необходимые инструменты не ограничены действием копирования соответствующих данных[1424]. Кроме того, существует целый ряд сопутствующих мер, которые необходимы для поддержания необходимой эффективности, например, извлечение самой компьютерной системы. Наиболее важным аспектом является сохранение целостности скопированных данных[1425]. Если следователи не имеют разрешения принять необходимые меры для обеспечения целостности скопированных данных, скопированные данные не могут быть приняты в качестве доказательств в уголовном судопроизводстве[1426]. После того как следователи скопировали данные и приняли меры для сохранения целостности, они должны будут решить, как поступить с исходными данными. В связи с тем, что следователи не будут перемещать аппаратные средства в ходе процесса извлечения, в целом информация будет оставаться там. Особенно в ходе расследований, связанных с незаконным содержанием[1427], например детской порнографии, следователи не смогут оставить данные на сервере. Поэтому им нужен инструмент, который позволит им удалять данные или, по крайней мере, обеспечить,

---

[1421] The importance of being able to extend the search to connected computer systems was already addressed by the Council of Europe Recommendation No. R (95) 13 of he Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543rd meeting of the Ministers Deputies. The text of the Recommendation is available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf

[1422] In this context it is important to keep in mind the principle of National Sovereignty. If the information are stored on a computer system outside the territory an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: “Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be 'in its territory”– Explanatory Report to the Convention on Cybercrime, No. 193. With regard to this issue see as well: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1423] For guidelines how to carry out the seizure of computer equipment see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1424] Regarding the classification of the act of copying the data see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 et seqq.

[1425] 'since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, 'maintain the integrity of the data', or maintain the ‘chain of custody’ of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data“. Explanatory Report to the Convention on Cybercrime, No. 197.

[1426] This principle also applies with regard to the seizure of hardware. Compared to maintaining the integrity of copied data it is often easier to maintain the integrity of data on a storage device.

[1427] See above: Chapter 2.5.

чтобы эти данные не могли быть доступны[1428]. Конвенция о киберпреступности касается вышеупомянутых вопросов в Статье 19 подпункт 3.

> ***Статья 19 – Поиск и извлечение хранимых компьютерных данных***
>
> *[…]*
>
> *3 Каждая Сторона принимает законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий производить извлечение или сходное с ним овладение компьютерными данными, доступ к которым был получен в соответствии с положениями параграфов 1 или 2. Эти меры должны включать предоставление полномочий:*
>
> *a) производить извлечение или сходное с ним овладение компьютерной системы, ее части или носителей, используемых для хранения компьютерных данных;*
>
> *b) изготавливать и оставлять у себя копии соответствующих компьютерных данных;*
>
> *c) обеспечивать целостность соответствующих хранимых компьютерных данных;*
>
> *d) делать компьютерные данные, находящиеся в компьютерной системе, доступ в которую был получен, недоступными или изымать их из нее.*

В этих случаях расследования сталкиваются со специфическими трудностями, поскольку они имеют международный характер, требующий международного сотрудничества в рамках расследования. Еще одной проблемой в отношении ордеров поиска компьютерных данных, является тот факт, что органам охраны правопорядка иногда сложно найти местонахождение данных. Зачастую они хранятся в компьютерных системах вне территории определенной страны. Даже тогда, когда известно точное местонахождение, объем хранимых данных часто мешает ускорить расследование[1429]. В этих случаях расследования сталкиваются со специфическими трудностями, поскольку они имеют международный характер, требующий международного сотрудничества в рамках расследования[1430]. Даже тогда, когда расследования проводятся касательно компьютерных систем, расположенных в пределах национальных границ, и следователи выявили поставщика услуг хостинга, управляющего серверами, на которых преступник хранит соответствующие данные, они могут столкнуться с трудностями в определении точного местоположения данных. Весьма вероятно, что даже малые и средние поставщика услуг хостинга имеют сотни тысяч серверов и жестких дисков. Зачастую следователи не смогут определить точное местоположение с помощью системного администратора, отвечающего за серверную инфраструктуру[1431]. Но даже если они не смогут определить конкретный жесткий диск, меры защиты могут удержать их от поиска соответствующих данных. Составители Конвенции решили этот вопрос введением принудительных мер для облегчения поиска и извлечения данных из компьютера. Подпункт 4 Статьи 19 позволяет следователям принудить системного администратора оказывать содействие органам охраны правопорядка. Несмотря на то, что обязанность следовать ордеру следователя ограничивается необходимой информацией и поддержкой для данного случая, этот инструмент изменяет характер процедур поиска и извлечения. Во многих странах ордеры на поиск и извлечение только заставляют людей, пострадавших в результате расследования, терпеть судебные разбирательства: они не должны активно поддерживать расследования. В отношении лица, обладающего специальными знаниями, необходимыми в ходе расследования, введение Конвенции о киберпреступности изменит ситуацию двумя путями. Прежде всего, они должны будут предоставить необходимую информацию следователям. Второе изменение связано с этим обязательством. Обязательство предоставлять разумную помощь следователям избавит лица, обладающие особыми знаниями, от договорных обязательств или ордеров, выданных

[1428] One possibility to prevent access to the information without deleting them is the use encryption technology.

[1429] See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

[1430] The fact, that the law enforcement agencies are able to access certain data, that are stored outside the country through a computer system in their territory does not automatically legalise the access. See Explanatory Report to the Convention on Cybercrime, No. 195. "This article does not address 'transborder search and seizure', whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation." Two cases of trans-border access to stored computer data are regulated in Art. 32 Convention on Cybercrime:
Article 32 – Trans-border access to stored computer data with consent or where publicly available
A Party may, without the authorisation of another Party:
a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[1431] "It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted." Explanatory Report to the Convention on Cybercrime, No. 200.

надзорными органами[1432]. Конвенция не определяет термин "разумный", но в Пояснительном Отчете указано, что разумный "*может включать раскрытие пароля или других мер безопасности следственным органам"*, но в целом не распространяется на *"раскрытие пароля или других мер безопасности"* когда это сопровождается *"неоправданной угрозой личной жизни других пользователей или другим данным, поиск которых не уполномочен вестись"*[1433].

> ***Статья 19 – Поиск и извлечение хранимых компьютерных данных***
>
> *[…]*
>
> *4 Каждая Сторона должна принимать законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий требовать от любого лица, обладающего знаниями о функционировании соответствующей компьютерной системы или применяемых мерах защиты хранящихся там компьютерных данных, предоставления в разумных пределах необходимых сведений, позволяющих осуществить действия, предусмотренные параграфами 1 и 2.*

Типовой закон Содружества о компьютерах и компьютерных преступлениях

Аналогичные подходы имеются и в Типовом законе Содружества от 2002 года[1434].

> ***Раздел 11***
>
> *В этой Части:*
>
> *[...]*
>
> *"извлекать" включает:*
>
> *a) создать и хранить копию компьютерных данных, в том числе с использованием местного оборудования; и*
>
> *b) делать компьютерные данные, находящиеся в компьютерной системе, доступ в которую был получен, недоступными или изымать их из нее; и*
>
> *c) распечатать вывод компьютерных данных.*

Раздел 12[1435]

1) Если следователь установил на основе [информации под присягой] [письменного показания под присягой], что существуют основания [подозревать] [полагать], что в таком месте может быть объект или компьютерные данные:

> *a) которые могут быть материальными доказательствами какого-либо преступления; или*
>
> *b) которые были приобретены лицом в результате преступления;*
>
> *судья [может] [должен] выдать ордер, уполномочивающий офицера [охраны правопорядка] [полиции], с такой помощью, которая может потребоваться, чтобы войти в указанное место для поиска и изъятия вещей и компьютерных данных.*

Раздел 13[1436]

> *1) Лицо, во владении или под контролем которого находится устройство хранения данных или компьютерная система, являющаяся объектом поиска в соответствии со Статьей 12, должно*

[1432] "A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data." Explanatory Report to the Convention on Cybercrime, No. 201.

[1433] Explanatory Report to the Convention on Cybercrime, No. 202.

[1434] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1435] Official Note: *If the existing search and seizure provisions contain a description of the content of the warrant, either in a section or by a form, it will be necessary to review those provisions to ensure that they also include any necessary reference to computer data.*

[1436] Official Note: *A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with ist constitutional or common law protections against self -incrimination.*

разрешить, и, в случае необходимости, оказывать помощь лицам, осуществляющим поиск, для того чтобы:

a) иметь доступ и использование компьютерной системы или устройства хранения данных компьютера для поиска каких-либо компьютерных данных, доступных для системы или в системе; и

b) получать и копировать такие компьютерные данные; и

c) использовать оборудования для создания копий; и

d) получить доступный для понимания вывод из компьютерной системы в обычном текстовом формате, который может быть прочтен.

2) Лицо, которое, не имея на то законных оправданий или оснований, разрешает или помогает другому лицу совершить преступление, наказывается, при осуждении к лишению свободы на срок не превышающий [период], либо штрафом не выше [сумма], или и то и другое.

6.2.7 Порядок производства

Даже если обязательство, сходное с упомянутым в подпункте 4 Статьи 19 Конвенции о киберпреступности не реализовано в национальном законодательстве, поставщики услуг часто сотрудничают с органами охраны правопорядка во избежание негативного влияния на свой бизнес. Если, по причине отсутствия сотрудничества со стороны поставщика услуг, следователям не удалось найти необходимые им для поиска и извлечения данные или устройства хранения, вполне вероятно, что следователям нужно извлечь больше аппаратных средств, чем необходимо в целом. Таким образом, поставщики услуг будут в целом поддерживать расследование и представлять соответствующие данные по запросу органов охраны правопорядка. Конвенция о киберпреступности содержит инструменты, позволяющие следователям воздержаться от ордеров поиска, если лицо, в распоряжении которого находятся соответствующие данные, передает их следователям[1437].

Несмотря на то, что совместные действия правоохранительных органов и поставщиков услуг, даже в отсутствие правовой основы, как представляется, являются положительным примером государственно-частного партнерства, существует целый ряд трудностей, связанных с нерегулируемым сотрудничеством. Кроме защиты данных, основная проблема связана с тем, что поставщики услуг могут нарушать договорные обязательства, взятые перед своими клиентами, если они выполняют запрос о представлении определенных данные, который не имеет достаточной правовой основы[1438].

Статья 18 – Порядок производства

1 Каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы предоставить ее компетентным органам полномочия требовать от:

a) лица на ее территории представить конкретные компьютерные данные, находящиеся во владении или под контролем этого лица, которые хранятся в компьютерной системе или на том или ином носителе компьютерных данных; и

b) поставщика услуг, предлагающего свои услуги на ее территории представить находящиеся во владении или под контролем этого поставщика услуг сведений о его абонентах.

Статья 18 содержит два обязательства. На основании подпункт 1a) Статьи 18 любое лицо, в том числе поставщик услуг, обязан представить определенные компьютере данные, находящиеся в его владении или под его контролем. В отличие от подпункта 1b), применение этого положения не ограничено конкретными данными. Термин "владение" предполагает, что лицо имеет физический доступ к устройствам хранения данных, где хранится указанная информация[1439]. Применение этого положения распространяется на термин "контроль". Данные находятся под контролем какого-либо лица, если он не имеет физического доступа, но управляет информацией. Это, например тот случай, когда подозреваемый хранит соответствующие данные

[1437] Regarding the motivation of the drafters see Explanatory Report to the Convention on Cybercrime, No. 171.

[1438] "A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability." Explanatory Report to the Convention on Cybercrime, No. 171.

[1439] Explanatory Report to the Convention on Cybercrime, No. 173.

на удаленной системе хранения данных с онлайновым доступом. Тем не менее, в Пояснительном отчете составители Конвенции отметили, что сами по себе технические возможности удаленного доступа к хранимым данным не являются необходимым установлением контроля[1440]. Применение Статьи 18 Конвенции о киберпреступности является ограниченным в тех случаях, когда степень контроля подозреваемого превышает потенциальную возможность доступа к нему.

Подпункт 1b) содержит порядок производства, который ограничивается определенными данными. На основании подпункта 1b) Статьи 18 следователи могут обязать поставщика услуг представить информацию об абоненте. Информация об абоненте может быть необходима для идентификации преступника. Если следователи смогут определить IP адрес, который был использован преступником, они должны привязать его к человеку[1441]. В большинстве случаев IP-адреса приводят только к поставщику услуг интернета, предоставившему IP-адрес пользователю. Перед активацией использования услуг поставщик услуг интернету, как правило, требует пользователя зарегистрироваться с помощью информации об абоненте[1442]. В этом контексте важно подчеркнуть, что Статья 18 Конвенции о киберпреступности не осуществляет и не внедряет ни обязательства по сохранению данных [1443], ни обязательство поставщиков услуг регистрировать информацию об абоненте[1444]. Подпункт 1b) Статьи позволяет следователям обязать поставщика услуг представить такую абонентскую информацию.

На первый взгляд не представляется необходимым делать различия между "компьютерными данными" в подпункте 1a) и " информацией об абоненте" в подпункте 1 b), так как информация об абоненте, которая хранится в цифровом виде, также охватывается подпунктом 1a). Первая причина для проведения различия связана с различными определениями "компьютерные данные" и "информация об абоненте". В отличие от "компьютерных данных", "информацию об абоненте" не требуется хранить в виде компьютерных данных. Подпункт 1 b) Статьи 18 Конвенции о киберпреступности предоставляет компетентным органам право представить информацию, которая хранится в нецифровой форме[1445].

> ***Статья 1 – Определения***
>
> *Для целей настоящей Конвенции:*
>
> *b) "компьютерные данные" означают любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные обязать компьютерную систему выполнять ту или иную функцию;*
>
> ***Статья 18 – Порядок производства***
>
> *3 Для целей настоящей Статьи термин " абонентская информация об абонентах" означает любую имеющуюся у поставщика услуг информацию о его абонентах в форме компьютерных данных или любой другой форме, кроме данных о трафике или содержании информации, и с помощью которой можно её установить:*
>
> *a) вид используемой услуги связи, принятые с этой целью меры технического обеспечения и период оказания услуги;*
>
> *b) личность абонента, его почтовый или географический адрес, номера телефона и других средств доступа, сведения о выставленных ему счетах и произведенных им платежах, имеющиеся в соглашении или договоре на обслуживание;*

[1440] "At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement." Explanatory Report to the Convention on Cybercrime, No. 173.
[1441] Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication see above: Chapter 3.2.12.
[1442] If the providers offer their service free of charge they do often either require an identification of the user nor do at least not verify the registration information.
[1443] See above: Chapter 6.2.5.
[1444] Explanatory Report to the Convention on Cybercrime, No. 172.
[1445] These can for example be information that were provided on a classic registration form and kept by the provider as paper records.

c) любые другие сведения о месте установки оборудования связи, имеющиеся в соглашении или договоре на обслуживание.

Второй причиной для проведения различия между "компьютерными данными" и "абонентской информацией" является тот факт, что это позволяет создателям законодательства вводить различные требования на применение этих инструментов[1446]. Это, например, возможность предъявлять более жесткие требования[1447] к порядку производства, относящегося к подпункту 1 b), поскольку эти инструменты позволяют органам охраны правопорядка получить доступ к любому виду компьютерных данных, в том числе данных содержания[1448]. Проведение различий между сбором данных о трафике в масштабе реального времени (Статья 20[1449]) и сбором данных о содержании в масштабе реального времени (Статья 21[1450]), показывает, что составители Конвенции осуществили, что, в зависимости от типа данных в этом вопросе, сотрудники органов охраны правопорядка получают доступ к различным гарантиям, которые должны быть выполнены[1451]. Устанавливая различия между "компьютерными данными" и "абонентской информацией", Статья 18 Конвенции о киберпреступности позволяет подписавшим ее государствам разработать аналогичную систему градационных гарантий в связи с порядком производства[1452].

Типовой закон Содружества о компьютерах и компьютерных преступлениях

Аналогичный подход имеется и в Типовом законе Содружества от 2002 года[1453].

Раздел 15

Если на основании заявления офицера полиции следователь установил, что определенные компьютерные данные в распечатанном либо ином виде представления информации, действительно необходимы для уголовного расследования или уголовного дела, следователь может постановить, что:

a) лицо на территории [постановляющей страны] под контролем компьютерной системы производит из системы указанные компьютерные данные либо в виде распечатки либо в другом понятном виде вывода данных; и

b) поставщик услуг интернет в [постановляющей стране] производит информацию о лицах, которые пользуются услугами на основе подписки или иной основе; и

c)[1454] лицо на территории [постановляющей страны], имеющее доступ к определенной компьютерной системе, обрабатывает и комплектует определенные компьютерные данные из системы и предоставляет их определенному лицу.

[1446] The Explanatory Report does even point out, that the parties to the Convention can adjust their safeguards with regard to specific data within each of the categories. See Explanatory Report to the Convention on Cybercrime, No. 174: “Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases“

[1447] For example the requirement of a court order.

[1448] The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 20) shows that the drafters of the Convention realised that the instruments are

[1449] See below: Chapter 6.2.9.

[1450] See below: Chapter 6.2.10.

[1451] Art. 21 Convention on Cybercrime obliges the signatory states to implement the possibility to intercept content data only with regard to serious offences (“Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law”). Unlike this Art. 20 Convention on Cybercrime is not limited to serious offences. “Due to the higher privacy interest associated with content data, the investigative measure is restricted to ‘a range of serious offences to be determined by domestic law’.” See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 230.

[1452] Regarding the advantages of a graded system of safeguards see above: Chapter 6.2.3..

[1453] “Model Law on Computer and Computer Related Crime”, LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1454] Official Note: *As noted in the expert group report, in some countries it may be necessary to apply the same standard for production*

6.2.8 Сбор данных в реальном масштабе времени

Прослушивание телефонных разговоров является инструментом, который используется во многих странах для расследования преступлений, за которые предусматривается смертная казнь[1455]. Многие правонарушения связаны с использованием телефона, особенно мобильного телефона, либо в процессе подготовки, либо при совершении преступления. В частности, в случаях, связанных с незаконным оборотом наркотиков, прослушивание разговоров между подозреваемыми могут иметь важное значение для успешного проведения расследования. Такое средство позволяет следователям собрать ценную информацию, хотя она ограничена обменом информацией по прослушиваемым линиям/телефонам. Если преступник использует другие средства обмена, например, письма или линии связи, которые не включены в прослушивание, следователям не удастся записать разговор. В общем ситуация такая же, когда идет о прямой разговор без использования телефона[1456].

В настоящее время обмен данными заменил классические телефонные разговоры. Обмен данными не ограничивается электронной почтой и передачей файлов. Увеличение количества голосовых сообщений осуществляется с помощью технологий, основанных на Интернет-протоколах (передача голоса по IP[1457]). С технической точки зрения, телефонный вызов по VoIP гораздо более сравним с обменом электронной почтой, чем классический телефонный вызов с помощью телефонного провода, и перехват такого вызовы сопровождается специфическими трудностями[1458].

Как и многие компьютерные преступления, включающие обмен данными, возможность в равной степени перехватывать эти процессы или иным образом использовать данные, связанные с процессом обмена, может стать одним из важнейших условий для успешного расследования. Применение существующих положений телефонного прослушиваниях, а также положений, связанных с использованием данными трафика электросвязи в расследовании киберпреступлений в некоторых странах столкнулось с трудностями. Трудности связаны с техническими вопросами[1459], также как и с правовыми. С юридической точки зрения, разрешение на запись телефонного разговора не обязательно включает разрешения на перехват процессов передачи данных.

Конвенция о киберпреступности нацелена закрыть существующие пробелы в способности органов охраны правопорядка контролировать процессы передачи данных[1460]. В рамках этого подхода, Конвенции о киберпреступности различает два вида наблюдения передачи данных. Статья 20 разрешает следователям для сбора данных о трафике. Термин "данные о трафике" определяется в Статье 1 d D) Конвенции о киберпреступности.

---

orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.
Official Note: *Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.*

[1455] Regarding the legislation on legal interception in Great Britain, Canada, South Africa, United States (New York) and Israel see: Legal Opinion on Intercept Communication, 2006, available at: http://www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

[1456] In these cases other technical solutions for the surveillance need to be evaluated. Regarding possible physical surveillance techniques see: *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997, page 384 et seqq.

[1457] Regarding the interception of VoIP to assist law enforcement agencies see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; Simon/Slay, Voice over IP: Forensic Computing Implications, 2006 - available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[1458] Regarding the interception of VoIP to assist law enforcement agencies see ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 48, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.htm*; Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; Simon/Slay, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[1459] Especially the missing technical preparation of Internet Providers to collect the relevant data in real-time.

[1460] Explanatory Report to the Convention on Cybercrime, No. 205.

Статья 1 – Определения

d) "данные о трафике" означают любые компьютерные данные, относящиеся к передаче информации посредством компьютерной системы, которые генерируются компьютерной системой, являющейся составной частью соответствующей цепи связи, и указывают на источник, назначение, маршрут, время, дату, размер, продолжительность или тип соответствующей услуги.

Различие между "данные содержания" и "данные о трафике" такое, какое проведение различия используется в большинстве национальных законов[1461].

6.2.9 Сбор данных о трафике

Конвенция о киберпреступности

В связи с тем, что определение данных о трафике различно в разных странах[1462], составители Конвенции о киберпреступности решили определить этот термин для совершенствования применения соответствующих положений международного расследования. Термин "данные о трафике" используется для описания данных, которые генерируются компьютерами во время процесса связи для маршрутизации соединения от источника до получателя. Всякий раз, когда пользователь подключается к интернету, генерируется трафик данных загрузки электронной почты или открытия веб-сайта. В связи с расследованиями киберпреступлений наиболее актуальны данные о трафике источника и получателя, являющиеся IP-адресами, которые идентифицируют партнеров по соединению в соединениях, использующих интернет[1463].

В отличие от "данных содержания" термин "данные о трафике" охватывает только данные, полученные в процессе передачи данных, но не сами переданные данные. Хотя доступ к данным содержания может в некоторых случаях оказаться необходимым, поскольку дает возможность правоохранительным органам охраны правопорядка гораздо более эффективным образом анализировать сообщения, трафик данных играет важную роль в расследовании киберпреступлений[1464]. При наличии доступа к данным содержания, что позволяет органам охраны правопорядка анализировать характер сообщений, обмен файлами, данные о трафике могут быть необходимы для выявления преступника. В случаях детской порнографии данные о трафике, например, могут позволить следователям определить веб-страницу, на которую преступник загружает изображения детской порнографии. Отслеживанием данных о трафике, получаемых при использовании услуг интернет, органы охраны правопорядка смогут определить IP-адрес сервера, а затем попытаться определить его физическое местонахождение.

Статья 20 – Сбор данных о трафике в режиме реального времени

1 Каждая Сторона должна принимать законодательные и иные меры, необходимые для предоставления ее компетентным органам полномочий:

a) собирать или записывать с применением технических средств на территории этой Стороны, и

b) обязать поставщиков услуг в пределах имеющихся у них технических возможностей:

i) собирать или записывать с применением технических средств на территории этой Стороны; или

ii) сотрудничать с компетентными органами и помогать им собирать или записывать в масштабе реального времени данные о трафике, связанные с конкретными сообщениями на территории этой Стороны, передаваемыми средствами компьютерной системы.

[1461] ABA International Guide to Combating Cybercrime, page 125.
[1462] ABA International Guide to Combating Cybercrime, page 125.
[1463] The "origin" refers to a telephone number, Internet Protocol (IP) address, or similar identification of a communications facility to which a service provider renders services. Explanatory Report to the Convention on Cybercrime, No. 30.
[1464] "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive." See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in Cybercrime investigations see as well: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 et seq.

2 Если какая-либо Сторона в силу устоявшихся принципов ее системы внутригосударственного права не может принять меры, предусмотренные параграфом 1 a), то вместо этого она может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в масштабе реального времени данных о потоках информации, связанных с указанными сообщениями, на ее территории путем применения технических средств на этой территории.

3 Каждая Сторона должна принимать законодательные и иные меры, необходимые для того, чтобы обязать поставщика услуг соблюдать конфиденциальность самого факта осуществления любых полномочий, предусмотренных настоящей статье, и любой информации об этом.

4 Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями Статей 14 и 15.

Статья 20 содержит два различных подхода к сбору данных о трафике, оба из которых должны быть выполнены[1465].

- Первый подход заключается в том, чтобы ввести обязательства поставщиков услуг интернета, дающие возможность органам охраны правопорядка непосредственно собирать соответствующие данные. Это в целом требует установки интерфейса, который органы охраны правопорядка могут использовать для доступа к инфраструктуре поставщиков услуг интернета[1466].
- Второй подход заключается в том, чтобы дать возможность органам охраны правопорядка, заставить поставщиков услуг интернета осуществлять сбор данных по запросу органов охраны правопорядка. Такой подход позволяет следователям сделать имеющимися в своем распоряжении существующие технические возможности и знания поставщиков в целом. Одно из намерений за сочетания двух подходов состоит в том, чтобы обеспечить, если поставщики не имеют на месте технологии для записи данных, органы охраны правопорядка должны иметь возможность проводить расследование (на основании подпункта 1b Статьи 20) без помощи от поставщика[1467].

Конвенция о киберпреступности разработана без предпочтения какой-либо конкретной технологии и без намерения установить стандарты, сопровождающиеся с необходимостью больших финансовых инвестиций в промышленность[1468]. С этой точки зрения подпункт 1a) Статьи 20 Конвенции о киберпреступности, как представляется, является лучшим решением. Вместе с тем, положение подпункта 2 Статьи 20 показывает, что составители Конвенции, сознавали, что некоторые страны могут столкнуться с трудностями в применении законодательства, позволяющего органам охраны правопорядка непосредственно проводить расследование.

Одной из основных трудностей в проведении расследований, основанных на Статье 20, является использование средств анонимной связи. Как указывалось выше[1469], преступники могут воспользоваться услугами сети интернет, позволяющими анонимную связь. Если преступник использует услуги анонимной связи, сходные с программным обеспечением TOR[1470], то в большинстве случаев следователи не в состоянии успешно анализировать данные о трафике и выявить партнера соединения. Преступник может достичь аналогичного результата с помощью терминалов доступа в интернет общего пользования[1471].

[1465] "In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a))." Explanatory Report to the Convention on Cybercrime, No. 223.

[1466] The Convention does not define technical standards regarding the design of such interface. Explanatory Report to the Convention on Cybercrime, No. 220.

[1467] Explanatory Report to the Convention on Cybercrime, No. 223.

[1468] "The article [Art. 20] does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Explanatory Report to the Convention on Cybercrime, No. 221.

[1469] See above: Chapter 3.2.12.

[1470] Tor is a software that enables users to protect against traffic analysis. For more information about the software see http://tor.eff.org/.

[1471] An example for an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of the Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorisation. In addition he is obliged to request an identification of his customers prior to the use of this services. Decree-Law 27 July 2005, no. 144. - Urgent measures for combating international terrorism. For more information about the Decree-Law see for example the article "Privacy and data retention policies in selected countries", available at http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

По сравнению с традиционными процедурами поиска и извлечения одним из преимуществ сбора данных о трафике является тот факт, что подозреваемый в совершении преступления не обязательно понимает, что проводится расследование[1472]. Это ограничивает его/ее возможности манипулирования или удаления доказательств. Для уверенности в том, чтобы преступники не были проинформированы поставщиком услуг интернета о проходящем расследовании, подраздел 3 Статьи 20 рассматривает этот вопрос и обязывает подписавшие государства ввести законодательство, обеспечивающее сохранность осведомленности о проводимом расследования конфиденциальной. Для поставщиков услуг это обстоятельство сочетается с тем преимуществом, что поставщик освобождается от обязательства[1473] информировать пользователей[1474].

Конвенция о киберпреступности была разработана в целях совершенствования и гармонизации законодательства в отношении вопросов, связанных с киберпреступностью[1475]. В этом контексте важно подчеркнуть, что на основе текста Статьи 21 Конвенции, это положение применяется не в отношении преступлений, связанных с киберпреступностью, но любого преступления. Относительно того факта, что использование электронных средств связи может иметь отношение не только к случаям киберпреступлений, применение этого положения вне киберпреступлений может быть полезными в рамках расследования. Что, например, позволит органам охраны правопорядка использовать данные о трафике, создаваемый в ходе обмена электронной почтой между преступниками для подготовки традиционного преступления. Подпункт 3 Статьи 14 позволяет сторонам делать оговорки и ограничения применения данного положения к некоторым преступлениям[1476].

Типовой закон Содружества о компьютерах и компьютерных преступлениях

Аналогичный подход имеется и в Типовом законе Содружества от 2002 года[1477].

> *1) Если офицер полиции установил, что данные о трафике, связанные с определенным соединением, действительно необходимы в целях уголовного расследования, офицер полиции может путем направления письменного уведомления лицу, под управлением которого находятся такие данные, потребовать от этого лица:*
>
> *a) собирать или записывать данные о трафике, связанные с указанным соединением в течение определенного периода; и*
>
> *b) разрешить и оказывать помощь указанному офицеру полиции в сборе и записи данных.*
>
> *2) Если следователь установил на основе [информации под присягой] [письменного показания под присягой], что существуют действительные основания [подозревать] [полагать], что данные о трафике действительно необходимы в целях уголовного расследования, следователь [может] [должен] уполномочить офицера полиции собирать или записывать данные о трафике, связанные с указанным соединением в течение определенного периода посредством применения технических средств.*

[1472] This advantage is also relevant for remote forensic investigations. See below: Chapter 6.2.12.

[1473] Such obligation might be legal or contractual.

[1474] Explanatory Report to the Convention on Cybercrime, No. 226.

[1475] Regarding the key intention see Explanatory Report on the Convention on Cybercrime No. 16: "The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation."

[1476] The drafters of the convention point out that the signatory states should limit the use of the right to make reservations in this context: Explanatory Report to the Convention on Cybercrime, No. 213.
Regarding the possibilities of making reservations see Art. 42 Convention on Cybercrime:
Article 42
By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

[1477] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

6.2.10 Перехват данных о содержании

Конвенция о киберпреступности

Помимо того факта, что структура Статьи 21 подобна Статье 20, она рассматривает данные о содержании. Возможность перехвата процессов обмена данных о содержании может быть важна в тех случаях, когда органы охраны правопорядка уже знают, кто сообщаются между собой партнеры, но не имеют никакой информации о типе обмениваемой информации. Статья 21 дает им возможность записывать данные соединения и анализировать содержание[1478]. Это включает файлы, загружаемые с веб-страниц или системы совместного доступа к файлам, отправленную или полученную преступником электронную почту и разговоры в чате.

> ***Статья 21 – Перехват данных о содержании***
>
> *1 Каждая Сторона принимает законодательные и иные меры в отношении ряда серьезных правонарушений, подлежащих квалификации в соответствии с нормами внутригосударственного права, необходимые для того, чтобы наделить ее компетентные органы полномочиями:*
>
> *a) собирать или записывать с применением технических средств на территории этой Стороны, и*
>
> *b) обязать поставщика услуг в пределах имеющихся у него технических возможностей:*
>
> *i) собирать или записывать с использованием технических средств на территории этой Стороны, или*
>
> *4 Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями Статей 14 и 15..*

В отличие от случая данных о трафике, Конвенция о киберпреступности не дает определения данным о содержании. Как указано в используемом термине "данные о содержании", это относится к содержанию сообщения.

Примеры данных о содержании в расследовании киберпреступлений, включают:

- предмет электронной почты;
- содержание веб-сайта, который был открыт подозреваемым;
- содержание разговора VoIP.

Одной из наиболее важных трудностей для расследований, основанных на Статье 21, является использование технологии шифрования[1479]. Как уже подробно объяснено выше, использование технологии шифрования

[1478] One possibility to prevent law enforcement agencies to analyse the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures see: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

[1479] Regarding the impact of encryption technology on computer forensic and criminal investigations see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: http://www.scm.uws.edu.au/compsci/computerforensics/ Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge see below: Chapter 6.2.11.

может позволить преступникам защищать передаваемое содержание таким образом, который делает невозможным получение органами охраны правопорядка доступа к нему. Если жертва зашифровала содержание, которое она передала преступникам, они могут только перехватить зашифрованное сообщение, но не проанализировать содержание. Без доступа к ключу, который был использован для шифрования файлов, возможность дешифровки может занять очень длительное время[1480].

Типовой закон Содружества о компьютерах и компьютерных преступлениях

Аналогичный подход имеется и в типовом законе Содружества 2002 года[1481].

> ***Перехват электронных сообщений***
>
> *18 1) Если [следователь] [судья] установил на основе [информации под присягой] [письменного показания под присягой], что существуют разумные основания [подозревать][полагать], что содержание электронных сообщений действительно требуется в целях расследования преступления, следователь [может] [должен]:*
>
> *a) обязать поставщика услуг интернет, чьи услуги доступны в [постановляющей стране] с применением технических средств, собирать или записывать, или разрешить или содействовать компетентным органам в сборе или записи данных о содержании, связанных с конкретными переданными сообщениями посредству компьютерной системы; или*
>
> *b) разрешить офицеру полиции собирать или записывать данные с применением технических средств.*

6.2.11 Правила, связанные с технологией шифрования

Как описано выше, преступники также могут препятствовать анализу данных о содержании, используя технологию шифрования. Доступны различные программные продукты, которые позволяют пользователям эффективно защитить файлы, а также процессы передачи данных от несанкционированного доступа[1482]. Если подозреваемые использовали определенные программные продукты и следственные органы не имеют доступа к ключу, который использовался чтобы зашифровать файлы, необходимая дешифровка может занять длительное время[1483].

Использование преступниками технологии шифрования является проблемой для органов охраны правопорядка[1484]. Существуют различные национальные и международные подходы[1485] к решению проблемы[1486]. Из-за различных оценок опасности от угрозы технологии шифрования до сих пор нет широко признанного международного подхода к решению этого вопроса. Наиболее распространенные решения:

[1480] *Schneier*, Applied Cryptography, Page 185.

[1481] "Model Law on Computer and Computer Related Crime", LMM(02)17; The Model Law is available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf.; Angers, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 et seq.; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1482] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1483] *Schneier*, Applied Cryptography, Page 185.

[1484] Regarding practical approaches to recover encrypted evidence see: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at:

[1485] The issue is for example addressed by Recommendation No. R (95) of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with information, 11 September 1995: "14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary." and the G8 in the 1997 Meeting in Denver: "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management, which may allow, consistent with these guidelines. Lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies. "

[1486] For more information see Koops, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

- В рамках уголовных расследований органы охраны правопорядка должны быть уполномочены взломать шифрование, если есть необходимость[1487]. Без такого разрешения или наличия возможности выпуска порядка производства, органы расследования могут оказаться не в состоянии собрать необходимые доказательства. Кроме того, или, как вариант, следователям может быть разрешено использовать ключевое программное обеспечение, чтобы перехватить зашифрованный файл для взлома шифрования[1488].

- Правила, которые ограничивают эффективность программного обеспечения для шифрования по средству ограничения длины ключа[1489]. Возможность следователей взломать ключ в течение разумного периода времени зависит от степени ограничения. Противники такого решения опасаются, что ограничения смогут взломать шифрование не только позволить следователям, но и шпионам, которые пытаются получить доступ к зашифрованной деловой информации[1490]. Кроме того, ограничение только помешает преступнику использовать криптостойкое шифрование, если такие программные инструменты не будут доступны. Это в первую очередь должны потребовать все международные стандарты, чтобы предотвратить производителя продуктов криптостойкого шифрования предлагать свое программное обеспечение в странах, не имеющих надлежащих ограничений в отношении длины ключа. В любом случае, преступники могли бы относительно легко создавать свое собственное программное обеспечение для шифрования, которое не ограничивает длину ключа.

- Обязательство создания системы депонированных ключей или процедур раскрытия ключа для продуктов криптостойкого шифрования[1491]. Реализация таких правил позволит пользователям продолжать использовать технологию криптостойкого шифрования, но и позволит следователям получить доступ к соответствующим данным, заставив пользователя предоставить ключ уполномоченным органам, тем самым сохранив ключ, предоставив его следователям при необходимости[1492]. Противники такого решения опасаются, что преступники смогут получить доступ к затребованным ключам и вместе с этим дешифровать секретную информацию. Кроме того, преступники могли бы сравнительно легко обойти правила путем разработки собственного программного обеспечения для шифрования, которое не требует предоставления ключа властям.

- Другим подходом является порядок производства[1493]. Этот термин описывает обязательства по раскрытию ключа, используемого для шифрования данных. Реализация данного инструмента обсуждалась в течение встречи в Денвере Группы восьми в 1997 году[1494]. Ряд стран ввели такие обязательства[1495]. Одним из примеров осуществления данного подхода на национальном уровне

[1487] The need for such authorisation if for example mentioned in principle 6 of the 1997 Guidelines for Cryptography Policy: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible."

[1488] This topic was discussed in the decision of the United States District Court of New Jersey in the case United States v. Scarfo. The District Court decided that the federal wiretapping law and the Fourth Amendment allow the law enforcement agencies to make use of a software to record the key strokes on the suspects computer (key logger) in order to intercept a passphrase to an encrypted file (if the system does not operate while the computer is communicating with other computers) See http://www.epic.org/crypto/scarfo/opinion.html

[1489] Export limitations for encryption software that is able process strong keys are not designed to facilitate the work of law enforcement agencies in the country. The intention of such regulations is to prevent the availability of the technology outside the country. For detailed information on import and export restrictions with regard to encryption technology see http://rechten.uvt.nl/koops/cryptolaw/index.htm.

[1490] The limitation of the import of such powerful software is even characterised as "misguided and harsh to the privacy rights of all citizens". See for example: The Walsh Report - Review of Policy relating to Encryption Technologies 1.1.16 available at: http://www.efa.org.au/Issues/Crypto/Walsh/walsh.htm

[1491] See: *Lewis*, Encryption Again, available at: http://www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

[1492] The key escrow system was promoted by the United States Government and implemented in France for a period of in 1996. For more information see Cryptography and Liberty 2000 – An International Survey of Encryption Policy. Available at: http://www2.epic.org/reports/crypto2000/overview.html#Heading9

[1493] See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 et seq.

[1494] "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management. which may allow, consistent with these guidelines. lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies.", http://www.g7.utoronto.ca/summit/1997denver/formin.htm.

[1495] See for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: http://www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf; Australia, Cybercrime Act, Art. 12, available at: http://scaleplus.law.gov.au/html/comact/11/6458/pdf/161of2001.pdf; Belgium, Wet van 28 november 2000 inzake informaticacriminaliteit, Art. 9 and Code of Criminal Procedure, Art. 88, available at:

является раздел 69 Закона об информационных технологиях Индии 2000 года[1496]. Одним из примеров такого обязательства является раздел 49 Закона о правовом регулировании следственных полномочий, принятый в 2000 году в Соединенном Королевстве[1497]:

Раздел 49

1) Настоящий раздел касается какой-либо защищенной информации, которая

a) становится или может стать собственностью какого-либо человека путем применения каких-либо законных прав на изъятие, удерживание, просмотр, поиск или иное вмешательство в документы или другую собственность;

b) становится или может стать собственностью какого-либо человека путем применения каких-либо законных прав на перехват связи;

c) становится или может стать собственностью какого-либо человека путем применения каких-либо прав, предоставленных разрешением в соответствии с разделом 22 3) или в соответствии с Частью II, либо в результате предоставления уведомления в соответствии с разделом 22 4);

d) становится или может стать собственностью какого-либо человека в результате того, что она была предоставлена или раскрыта для совершения каких-либо законных действий (независимо от того, было ли это результатом запроса или нет);

e) может какими-нибудь другими законными средствами, не вовлекающими применение законных прав, вовлекать во владение какими-либо интеллектуальными услугами полицию, таможню и акцизную службу или выполнять действия, схожие с вовлечением к владению каких-либо этих услуг полиции, таможни и акцизной службы.

2) Если какое-нибудь лицо с соответствующим разрешением, согласно перечню 2, считает с достаточными основаниями

a) что ключ к защищенной информации находится у какого-либо лица,

b) что наложение требования раскрытия информации в отношении защищенной информации i), необходимо по причине, попадающей в подраздел 3), или ii), необходимо для обеспечения защиты эффективного применения или надлежащего исполнения каким-либо государственным органом какого-либо законного права или законных обязанностей,

---

http://staatsbladclip.zita.be/staatsblad/wetten/2001/02/03/wet-2001009035.html; France, Loi pour la confiance dans l'économie numérique, Section 4, Artikel 37, available at: http://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B78A2A8ED919529E3B420C082708C031.tpdjo12v_3?cidTexte=JORFTEXT000000801164&dateTexte=20080823; United Kingdom, Regulation of Investigatory Powers Act 2000, Art. 49, available at: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: http://www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: http://www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: http://www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative a l'echange electronique de donnees juridiques, Chapter. III, available at: http://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/; Netherlands, Wet op de inlichtingen en veiligheidsdiensten 2002, Art. 89, available at http://www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: http://www.info.gov.za/gazette/acts/2002/a70-02.pdf;Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: http://www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

[1496] An example can be found in Sec. 69 of the Indian Information Technology Act 2000: "Directions of Controller to a subscriber to extend facilities to decrypt information.(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information." For more information about the Indian Information Technology Act 2000 see Duggal, India's Information Technology Act 2000, available under: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf

[1497] For general information on the Act see: *Brown/Gladman*, The Regulation of Investigatory Powers Bill - Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses, available at: http://www.fipr.org/rip/RIPcountermeasures.htm; *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm; ABA International Guide to Combating Cybercrime, page 32.

c) что наложение такого требования соразмерно с тем, чего стремились достичь путем его наложения, и

d) что нет обоснованной пользы для какого-либо лица с соответствующим разрешением получить право владения защищенной информацией в доступной форме без предоставления уведомления в соответствии с настоящим разделом, лица с этим разрешением, который может путем уведомления лица, которому он доверяет получить во владение ключ, наложить требование о раскрытии защищенной информации.

3) По условиям данного подраздела для раскрытия какой-либо защищенной информации необходимо требование о раскрытии информации, если это необходимо

a) в интересах национальной безопасности;

b) для предотвращения или выявления преступления; или

c) в интересах экономического благосостояния Соединенного Королевства.

4) В соответствии с настоящим разделом уведомление, налагающее требование о раскрытии какой-либо защищенной информации

a) должно быть сделано в письменной форме или (если не в письменной форме) должно быть сделано в такой форме, которая покажет запись о том, что оно получено;

b) должно описывать защищенную информацию, к которой имеет отношение уведомление;

c) должно перечислить вопросы, входящие в подраздел 2)b)i) или ii), со ссылкой на выданное уведомление;

d) должно указывать должность, звание или положение того лица, которое его выдало;

e) должно указывать должность, звание или положение того лица, кому в соответствии с перечнем 2, предоставлено уведомление или (если лицо, выдающее уведомление имело право выдавать его без разрешения другого человека), необходимо изложить обстоятельства, при которых возникло это право;

f) должно указывать время, в течение которого должно быть выполнено уведомление; и

g) должно содержать тот факт, что раскрытие требуется в соответствии с уведомлением, в форме и в порядке, в котором оно должно быть произведено, а также срок, установленный для задач пункта f), должно определять срок выполнения, который является разумным при всех обстоятельствах.

Для обеспечения того, чтобы лицо, обязанное раскрыть ключ в приказном порядке, выполнило приказ и действительно предоставило настоящий ключ, Закон Соединенного Королевства о правовом регулировании следственных полномочий, принятый в 2000 году, содержит положение, которое квалифицирует невыполнение такого приказа как преступление.

Раздел 53

1) Лицо, которому в разделе 49 предъявлено уведомление, является виновным в совершении преступления, если после направления уведомления он сознательно не исполнил раскрытие в соответствии с уведомлением.

2) При слушаниях против какого-либо лица за совершение преступления в соответствии с данным разделом, если будет доказано, что лицо обладало ключом к какой-либо защищенной информации в течение какого-либо времени перед тем, как ему было выдано уведомление из раздела 49, это лицо должно в целях этого расследования по-прежнему иметь этот ключ в распоряжении на протяжении времени, пока не доказано, что ключ не был в его владении после вручения уведомления и до момента, когда оно было обязано его раскрыть.

3) В целях настоящего раздела человек должен быть взят, с тем чтобы показать, что он не владел ключом к защищенной информации в течение определенного времени, если

a) представлено достаточное количество фактов, чтобы поднять вопрос по отношению к этому; и

b) обратное не подтверждается ни одним разумным доводом.

4) На слушаниях против любого лица за преступление, согласно данному разделу, должна быть защита для человека, чтобы показать,

a) что действительно он не мог совершить требуемое раскрытие на основании выданного уведомления раздела 49 до конца требуемого времени, указанного в этом уведомлении; и

b) что раскрытие произошло в скором времени после того времени, которое считалось достаточным для этого раскрытия.

5) Лицо, виновное в совершении преступления, согласно данному разделу подлежит,

a) в случае обвинительного заключения, осуждению на срок, не превышающий двух лет, или наложению штрафа, или применению обоих наказаний;

b) при обвинительном заключении без участия присяжных осуждению на срок, не превышающий шести месяцев или наложению штрафа, или применению обоих наказаний.

Закон о правовом регулировании следственных полномочий 2006 года обязывает подозреваемого в совершении преступления, поддерживать работу органов охраны правопорядка. Существуют три основные проблемы, связанные с этим положением:

- Общая озабоченность связана с тем фактом, что обязательство ведет к потенциальному конфликту с основополагающими правами подозреваемого в отношении самого себя[1498]. Вместо того, чтобы оставить расследование компетентным органам, подозреваемому необходимо активно поддерживать расследование. Сильная защита от самого себя во многих странах вызывает в настоящее время вопрос, в какой мере такое регулирование имеет возможность стать моделью решения проблем, связанных с технологией шифрования.
- Еще одна проблема связана с тем фактом, что потерянный ключ может привести к уголовному расследованию. Несмотря на то, что уголовная ответственность предполагает, что преступник сознательно отказывается раскрыть утраченный ключ, это вовлекает людей, использующих ключ шифрования, в ненужные уголовные процессы. Но особенно раздел 53 подпункт 2 теоретически препятствует бремени доказывания[1499].

[1498] Regarding the discussion about the protection against self-incrimination under the United States law see for example: *Clemens*, No Computer Exception to the Constitution: The First Amendment Protects Against Compelled Production of an Encrypted Document or Private key, UCLA Journal of Law and Technology, Vol. 8, Issue1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: http://www.richmond.edu/jolt/v2i1/sergienko.html; *O'Neil*, Encryption and the First Amendment, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: http://www.vjolt.net/vol2/issue/vol2_art1.pdf; *Fraser*, The Use of Encrypted, Coded and Secret Communication is an "Ancient Liberty" Protected by the United States Constitution, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: http://www.vjolt.net/vol2/issue/vol2_art2.pdf; Park, Protecting the Core Values of the First Amendment in an age of New Technology: Scientific Expression vs. National Security, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: http://www.vjolt.net/vol2/issue/vol2_art3.pdf; Hearing before the Subcommittee on the Constitution, Federalism, and Property Rights of the Committee on the Judiciary, United States Senate, 150 Congress, Second Session on Examining the Use of Encryption, available at: http://www.loc.gov/law/find/hearings/pdf/00139296461.pdf.
Regarding the discussion in Europe about self-incrimination, in particular with regard to the European Convention on Human Right (ECHR) see *Moules*, The Privilege against self-incrimination and the real evidence, The Cambridge Law Journal, 66, page 528 et seq.; *Mahoney*, The Right to a Fair Trail in Criminal Matters under Art. 6 ECHR, Judicial Studies Institute Journal, 2004, page 107 et seq.; *Birdling*, Self-incrimination goes to Strasbourg: O'Halloran and Francis vs. United Kingdom, International Journal of Evidence and Proof, Vol. 12, Issue 1, 2008, page 58 et seq.; Commission of the European Communities, Green Paper on the Presumption of Innocence, COM (2006) 174, page 7, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0174:FIN:EN:PDF.

[1499] In this context see as well: Walker, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: http://www.bileta.ac.uk/01papers/walker.html.

- Существуют технические решения, которые позволяют преступникам обходить обязательство раскрытия ключа, используемого для шифрования данных. Одним из примеров того, каким образом преступник может обойти обязательство является использование программного обеспечения для шифрования, основанного на принципе "достоверного отрицания возможности"[1500].

6.2.12 Программное обеспечение удаленной судебной экспертизы

Как пояснено выше, поиск доказательства на компьютере подозреваемого требует физического доступа к соответствующему оборудованию – компьютерной системе и внешнему запоминающему устройству. Эта процедура в целом сопровождается необходимостью получения доступа в квартиру, дом или офис подозреваемого. В этом случае подозреваемый будет осведомлен о продолжающемся расследовании в тот момент, когда следователи начали проведения поиска[1501]. Эта информация может привести к изменению в поведении[1502]. Если преступник, например, нападал на несколько компьютерных систем, чтобы тестировать свои возможности в практических целях для подготовки гораздо более крупных серий нападений в будущем вместе с другими преступниками, то процедура поиска мешала следователям установить других подозреваемых, так как вероятно, что преступник прекратит с ними связь.

Чтобы избежать обнаружения продолжающихся расследований, органы охраны правопорядка требуют инструмент, который разрешает им получить доступ к компьютерным данным, хранящим расчеты подозреваемого, которые могли тайно использоваться подобно телефонному наблюдению для мониторинга телефонных звонков[1503]. Такой инструмент позволил бы органам охраны правопорядка получить удаленный доступ к компьютеру подозреваемого и искать информацию. В настоящее время вопрос, необходимы ли такие инструменты или нет, интенсивно обсуждался[1504]. Уже в докладах 2001 года отмечалось, что ФБР Соединенных Штатов разработало клавиатурный шпион, как инструмент для расследований, связанных с интернетом под названием "волшебный фонарь"[1505]. В 2007 году были опубликованы доклады, что органами охраны правопорядка в Соединенных Штатах использовалось программное обеспечение для отслеживания преступников, которые используют средства анонимной связи[1506]. В докладах были ссылки на ордер на право обыска, где использование инструмента, называемого CIPAV[1507], было затребовано[1508]. После того,

---

[1500] Regarding possibilities to circumvent the obligations see *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm.

[1501] A detailed overview about the elements of search procedures as well as the challenges of carrying them ot is provided by the ABA International Guide to Combating Cybercrime, 123 et seq. For more information on Computer-related Search and Seizure see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 et seqq.; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 et seqq.

[1502] Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an on going investigation based on Art. 20 confidential see above: Chapter 6.2.9.

[1503] There are disadvantages related to remote investigations. Apart from the fact that direct access enables the law enforcement agencies to examine the physical condition of storage media physical access to a computer system it is the only way to ensure that the files on the suspects computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[1504] Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: http://www.news.com/8301-10784_3-9769886-7.html.

[1505] See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf ; *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 et seq., available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf; Green, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: http://www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.200, available at: http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: http://www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; Abreu, FBI confirms "Magic Lantern" project exists, 2001, available at: http://www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

[1506] See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: http://www.news.com/8301-10784_3-9746451-7.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf; Secret online search warrant: FBI uses CIPAV for the first time, Heise News, 19.07.2007, available at: http://www.heise-security.co.uk/news/92950.

[1507] Computer and Internet Protocol Address Verifier.

[1508] A copy of the search warrant is available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf. Regarding the result of the search see: http://www.politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf; For more information about CIPAV see: *Keizer*, What we know

как Федеральный суд Германии постановил, что существующее уголовно-процессуальное право не позволяет следователям использовать программное обеспечение удаленной судебной экспертизы для тайного поиска данных в компьютере подозреваемого, началась дискуссия о необходимости внести поправки в существующие законы в этой области[1509]. В ходе дискуссии была опубликована информация, что органы расследования незаконно использовали программное обеспечение удаленной судебной экспертизы в ходе пары расследований[1510].

Обсуждались[1511] различные концепции "программного обеспечения удаленной судебной экспертизы" и особенно его возможные функции. С теоретической точки зрения программное обеспечение может иметь следующие функции:

- Функция поиска – эта функция позволит органам охраны правопорядка искать незаконное содержание и собирать информацию о файлах, хранящихся в компьютере[1512].
- Записи – следователи смогут записывать данные, которые обрабатываются в компьютерной системе подозреваемого без постоянного хранения. Если подозреваемый, например, использует услуги VoIP для установления связи с другими подозреваемыми, содержание разговора, в общем, не сохранится[1513]. Программное обеспечение удаленной судебной экспертизы сможет записать обрабатываемые данные, чтобы сохранить их для следователей.
- Клавиатурного шпиона – если программное обеспечение удаленной судебной экспертизы содержит модуль, который записывает нажатия клавиатуры, этот модуль может использоваться для записи паролей, который подозреваемый использует для шифрования файлов[1514].
- Идентификации – эта функция позволит доказать следователям, что подозреваемый участвовал в уголовном преступлении, даже если он использовал услуги анонимной связи, которые мешают следователям выявить преступника, отслеживающего используемые IP-адреса[1515].
- Активации внешних устройств – может быть использовано удаленное программное обеспечение для включения веб-камеры или микрофона комнате наблюдения[1516].

Несмотря на то, что возможные программные функции, которые представлены, будет очень полезны для следователей, важно указать на то, что существует целый ряд правовых, а также технических трудностей, связанных с использованием такого программного обеспечения. С технической точки зрения, должны быть приняты во внимание следующие аспекты:

(now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: http://www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV fort he first time, Heise Security News, 19.07.2007, available at: http://www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: http://www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: http://www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

[1509] Regarding the discussion in Germany see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: http://www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: http://www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html; *Leyden*, Germany seeks malware 'specialists" to bug terrorists, The Register, 21.11.2007, available at: http://www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/; Berlin's Trojan, Debate Erupts over Computer Spying, Spiegel Online International, 30.08.2007, available at: http://www.spiegel.de/international/germany/0,1518,502955,00.html

[1510] See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: http://www.tagesspiegel.de/politik/;art771,1989104.

[1511] For an overview see *Gercke*, Secret Online Search, Computer und Recht 2007, page246 et seq.

[1512] The search function was in the focus of the decision of the German Supreme Court in 2007. See: Online police searches found illegal in Germany, 14.02.2007, available at: http://www.edri.org/edrigram/number5.3/online-searches.

[1513] Regarding investigations involving VoIP see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at http://www.itaa.org/news/docs/CALEAVOIPreport.pdf; Simon/Slay, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[1514] This is the focus of the FBI software "magic lantern". See: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 et seq., available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf; See also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1515] This is the focus of the US investigation software CIPAV. Regarding the functions of the software see the search warrant, available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf.

[1516] Regarding this functions see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 et seq.

- Трудности, связанные с процессом установки, – программное обеспечение должно быть установлено на компьютерную систему подозреваемого. Распространение вредоносного программного обеспечения доказывает, что установка программного обеспечения на компьютер пользователя интернета без его разрешения невозможно. Но главная разница между вирусом и программным обеспечением удаленной судебной экспертизы фактически заключается в том, что программное обеспечение удаленной судебной экспертизы необходимо установить на конкретную компьютерную систему (компьютер подозреваемого), в то время как компьютерный вирус стремится заразить столько компьютеров, насколько это возможно, без нацеливания на конкретную компьютерную систему. Существует несколько способов, как программное обеспечение может быть передано на компьютер подозреваемого. Например, установка с физическим доступом к компьютерной системе; размещение программного обеспечения на веб-сайте для скачивания; доступ онлайн к компьютерной системе в обход мер безопасности, а также программное обеспечение, скрытое в потоке данных, создаваемых в ходе деятельности в интернете, это лишь несколько примеров[1517]. Поскольку защитными мерами, такими как средства обнаружения вирусов и брандмауэры, оснащено большинство компьютеров, для следователей наряду со всеми методами удаленной установки существует и ряд трудностей[1518].
- Преимущество физического доступа – проводится целый ряд анализов, например, физическая проверка средства обработки данных, требует доступа к оборудованию. Кроме того, программное обеспечение удаленной судебной экспертизы позволило бы следователям только анализировать компьютерные системы, подключенные к интернету[1519]. Более того, очень трудно сохранить целостность компьютерной системы подозреваемого[1520]. В отношении этих аспектов программное обеспечение удаленной судебной экспертизы, в целом, не сможет заменить физический осмотр компьютерной системы подозреваемого.

Кроме того, перед выполнением данного положения необходимо принять во внимание ряд правовых аспектов, которые позволят следователям установить программное обеспечение удаленной судебной экспертизы. Гарантии, установленные в Уголовно-процессуальных кодексах, также как и Конституции многих стран, ограничивают потенциальные функции такого программного обеспечения. В дополнение к национальным аспектам установка программного обеспечения удаленной судебной экспертизы могут нарушать принцип национального суверенитета[1521]. Если программное обеспечение установлено на ноутбук, который вывезен из страны после процесса установки, программное обеспечение может дать следователям возможность осуществлять уголовное расследование на территории иностранного государства без соответствующего разрешения компетентных органов.

6.2.13 Требование авторизации

Преступники могут принимать определенные меры, чтобы осложнить расследование. В дополнение к использованию программного обеспечения, которое позволяет использовать анонимную связь[1522], идентификация может оказаться сложной, если подозреваемый использует общедоступный терминал выхода в интернет или открытые беспроводные сети. Ограничения на производство программного обеспечения, которое позволяет пользователю скрыть его/ее обнаружение и сделать доступным общедоступный терминал выхода в интернет, который не требует идентификации, может позволить органам охраны правопорядка проводить расследования более эффективно. Примером такого подхода к ограничению использования общедоступных терминалов для совершения уголовных преступлений, является Статья 7[1523] итальянской Директивы 144[1524],

---

[1517] Regarding the possible ways for an infection of a computer system by a spyware see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: http://www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.

[1518] With regard to the efficiency of virus scanners and protection measures implemented in the operating systems it is likely that the functioning of a remote forensic software would require the cooperation of software companies. If software companies agree to prevent a detection of the remote forensic software this could go along with serious risks for the computer security. For more information see *Gercke*, Computer und Recht 2007, page 249.

[1519] If the offender stores illegal content on an external storage device that is not connected to a computer system the investigators will in general not be able to identify the content if they do just have access to the computer system via a remote forensic software.

[1520] With regard to the importance of maintaining the integrity during a forensic investigation see *Hosmer*, Providing the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, Vol. 1, Issue 1, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[1521] National Sovereignity is a fundamental principle in International Law. See Roth, State Sovereignity, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

[1522] See above: Chapter 3.2.12.

[1523] Based on Art. 7 "anyone running an establishment open to the public or any kind of private association where devices or terminals, which can be used for electric data transmission or other communications, are made available to the public, to customers or members" is obliged to require a licensce by local authorities and identify persons using the service. For more information see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 et seq

которая была преобразована в закон в 2005 году (Legge № 155/2005[1525]). Это условие вынуждает любого, кто намеревается предоставить общественный доступ в интернет (например, интернет-кафе или университеты[1526]) подать заявку на авторизацию. Кроме того, человек обязан запросить требование к идентификации от его/ее клиентов до предоставления им доступа к использованию услуги. В связи с тем фактом, что частное лицо, устанавливающее беспроводную точку доступа, как правило, не охвачено этим обязательством, может быть возможность довольно легко обойти наблюдение, если преступники используют незащищенные частные сети, с тем чтобы скрыть свою личность[1527].

Можно усомниться в том, оправдывает ли степень улучшения расследований ограничение доступа в интернет и услугам анонимной связи. Бесплатный доступ в интернет сегодня признан в качестве важного аспекта такого, как право на свободный доступ к информации, которое защищается конституцией в ряде стран. Вполне вероятно, что требования к идентификации будут влиять на использование интернета, так как пользователи будут всегда бояться, что их использование интернета просматривается. Даже тогда, когда пользователи знают, что их действия законны, это все еще может повлиять на их взаимодействие и использование[1528]. В то же время, преступники, которые хотят предотвратить идентификацию могут легко обойти процедуру идентификации. Они могут, например, использовать телефонные карты предоплаты, купленные за границей, которые не требуют идентификации для доступа в интернет.

6.3 Международное сотрудничество

6.3.1 Введение

Все большее число киберпреступлений имеют международный масштаб[1529]. Как отмечалось выше, одна из причин этого явления заключается в том, что существует очень малая необходимость физического присутствия лица, совершившего преступление в месте, где предоставляется услуга[1530]. Как следствие, преступники, в общем случае, не должны присутствовать там, где находится жертва. В общем, расследования киберпреступлений продвигаются с необходимостью международного сотрудничества[1531]. Одним из ключевых требований следователей в транснациональных расследованиях является немедленная реакция коллег в стране нахождения преступника[1532]. Особенно, когда это относится к проблеме отсутствия традиционных инструментов взаимопомощи, в большинстве случаев выполнить требования в отношении скорости расследований в интернете[1533]. Конвенция о киберпреступности уделяет все более важное значение международному сотрудничеству в Статьях с 23 по 35. Другой подход содержится в проекте Стэнфордской конвенции[1534].

[1524] Decree 144/2005, 27 July 2005 ("Decreto-legge"). – Urgent measures for combating international terrorism. For more information about the Decree-Law see for example the article Privacy and data retention policies in selected countries available at http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[1525] For more details see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 et seq.

[1526] *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

[1527] Regarding the related challenges see: *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime" in Cybercrime & Security, IIA-2, page 6 et seq.

[1528] *Büllingen/Gillet/Gries/Hillebrand/Stamm*, Situation and Perspectives of Data Retention in an international comparison (Stand und Perspectiven der Vorratsdatenspeichung im internationalen Vergleich, 2004, page 10, available at: http://www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

[1529] Regarding the transnational dimension of Cybercrime see: Keyser, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf.
Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension - in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et seq., available at: http://media.hoover.org/documents/0817999825_1.pdf;

[1530] See above: Chapter 3.2.7.

[1531] See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol 9, page 451 et seq., available at: http://www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

[1532] *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

[1533] The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[1534] See below: Chapter 6.3.9.

6.3.2 Общие принципы международного сотрудничества

Статья 23 Конвенции о киберпреступности определяет три основные принципа, касающиеся международного сотрудничества в расследовании киберпреступлений среди ее членов.

> ***Статья 23 – Общие принципы, касающиеся международного сотрудничества***
>
> *Стороны сотрудничают друг с другом в соответствии с положениями настоящей главы, а также путем применения соответствующих международных документов о международном сотрудничестве по уголовным делам, договоренностям, достигнутым на основе единообразного или взаимообязывающего законодательства и внутренних законов в максимально возможной степени в целях проведения расследований или разбирательств, касающихся уголовных преступлений, связанных с компьютерными системами и данными, или для сбора в электронной форме доказательств уголовного преступления.*

Во-первых, предполагается, что участники обеспечивают наиболее широкое сотрудничество в области международного расследования. Это обязательство отражает важность международного сотрудничества в расследовании киберпреступлений. Кроме того, Статья 23 отмечает, что общие принципы применимы не только в расследовании киберпреступлений, а в любых расследованиях с необходимостью сбора доказательств в электронной форме. Это включает расследование киберпреступлений, а также расследования в традиционных случаях. Если подозреваемый в убийстве использовал услугу электронной почты за рубежом, Статья 23 будет применяться в отношении расследований, связанных с данными, хранимыми поставщиком услуг хостинга[1535]. Третий принцип отмечает, что положения, касающиеся международного сотрудничества, не подменяют положений международных соглашений, в том, что касается взаимной правовой помощи и экстрадиции или соответствующих положений внутреннего законодательства, касающихся международного сотрудничества. Составители Конвенции подчеркивают, что взаимопомощь должна в целом осуществляется на основе применения соответствующих договоров и аналогичных соглашений о взаимопомощи. Как следствие, Конвенция не намерена создать отдельный общий режим взаимопомощи. Таким образом, только в тех случаях, когда существующие договоры, законы и механизмы еще не содержат таких положений, каждая Сторона должна создать правовую основу для осуществление международного сотрудничества, как ни определено в Конвенции[1536].

6.3.3 Экстрадиция

Экстрадиция граждан остается одной из самых трудных аспектов международного сотрудничества[1537]. Запросы об экстрадиции очень часто приводят к конфликту между необходимостью защитить граждан и необходимостью оказывать поддержку проводимого расследования в зарубежной стране. Статья 24 определяет принципы экстрадиции. В отличие от Статьи 23 это положение ограничено в отношении правонарушений, указанных в Конвенции, и не применяется в случаях, являющихся незначительными (лишение свободы на максимальный срок не менее одного года[1538]). Во избежание конфликтов, которые могут возникнуть с учетом способности Сторон делать оговорки, Статья 24 основана на принципе двойной уголовной ответственности[1539].

> ***Статья 24 – Экстрадиция***
>
> *1a) Эта статья применяется к экстрадиции между Сторонами за уголовные преступления, признанные таковыми в соответствии со Статьями 2 по 11 настоящей Конвенции, при условии*

[1535] See Explanatory Report to the Convention on Cybercrime, No. 243. The Member States have the possibility to limit the international cooperation with regard to certain measures (extradition, real time collection of traffic data and the interception of content data).
[1536] If for example two countries involved in a cybercrime investigation already do have bilateral agreements in place that contain the relevant instruments, this agreement will remain a valid basis for the international cooperation
[1537] Regarding the difficulties related to the dual criminality principle see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 et seqq., available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.
[1538] The Explanatory Report clarifies that the determination of the covered offences does not depend on the actual penalty imposed in the particular cases. See: Explanatory Report to the Convention on Cybercrime, No. 245.
[1539] Regarding the dual criminality principle see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 et seqq., available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

что они являются наказуемыми в соответствии с законодательством обеих Сторон в виде лишения свободы на срок не менее одного года, либо на более строгое наказание.

b) В случаях разных минимальных наказаний, которые должны применяться в соответствии с договоренностью на основе единообразного либо взаимообязывающего законодательства или договора о выдаче, включая Европейскую конвенцию об экстрадиции (ETS № 24), применяемых между двумя или более сторонами, должно применяться минимальное наказание, предусмотренное в рамках такого соглашения или договора.

2 Уголовные правонарушения, указанные в пункте 1 настоящей статьи, должны быть включены в качестве преступлений, влекущих экстрадицию, в любой договор о выдаче, заключенный между Сторонами. Стороны обязуются включать такие правонарушения в качестве преступлений, влекущих выдачу, в любой договор о выдаче, заключаемый между ними.

3 Если Сторона, обуславливающая экстрадицию наличием договора, получает запрос на экстрадицию от другой Стороны, с которой не имеет договора об экстрадиции, она может рассматривать настоящую Конвенцию в качестве правовой основы для экстрадиции в связи с любым уголовным преступлением, упомянутым в пункте 1 настоящей статьи.

4 Стороны, не обуславливающие экстрадицию наличием договора, признают между собой уголовные преступления, упомянутые в пункте 1 настоящей статьи, в качестве преступлений, влекущих экстрадицию.

5 Экстрадиция осуществляется с соблюдением условий, предусмотренных законодательством запрашиваемой Стороны или применимыми договорами об экстрадиции, включая основания, при которых запрашиваемая Сторона может отказать в выдаче.

6 Если в выдаче за совершение уголовного преступления, указанного в пункте 1 настоящей статьи, отказано исключительно на основании гражданства разыскиваемого лица или потому, что запрашиваемая сторона полагает, что он обладает юрисдикцией в отношении преступления, запрашиваемая Сторона должна передать дело по просьбе запрашивающей Стороны своим компетентным органам для целей уголовного преследования и должна сообщить окончательный результат запрашивающей Стороне в установленном порядке. Эти органы принимают решения и проводят расследования и судебные разбирательства в том же порядке, что и для любого другого преступления сопоставимого характера в соответствии с законами этой Стороны.

7 a) Каждая Сторона должна в момент подписания или в момент сдачи на хранение своего правового акта ратификации, принятия, одобрения или присоединения сообщить Генеральному секретарю Совета Европы название и адрес каждого органа, ответственного за осуществление или получение запроса об экстрадиции или предварительном аресте в отсутствие договора.

b) Генеральный Секретарь Совета Европы должен создать и хранить обновленный реестр уполномоченных органов, назначенных Сторонами. Каждая Сторона гарантирует, что сведения, содержащиеся в регистре, верны все время.

6.3.4 Общие принципы взаимопомощи

Относительно взаимопомощи, Статья 25 дополняет принципы, изложенные в Статье 23. Одним из наиболее важных положений Статьи 25 является пункт 3, в котором подчеркивается важность быстрой связи в расследовании киберпреступлений[1540]. Как отмечалось ранее, ряд расследований киберпреступлений на национальном уровне провалился по причине того, что расследования шли слишком долго и важные данные были удалены, прежде чем процедурными мерами предписали сохранить их и изъять[1541]. Расследования,

[1540] See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[1541] See above: Chapter 3.2.10.

которые требуют оказания взаимной правовой помощи в целом занимают еще больше времени из-за занимающих время формальных требований по установлению связи с органами охраны правопорядка. Конвенция решает эту проблему, подчеркнув важность создания условий для ускоренного использования средств коммуникации[1542].

Статья 25 – Общие принципы, касающиеся взаимопомощи

1 Стороны оказывают друг другу взаимопомощь в максимально возможной степени в целях проведения расследований или разбирательств, касающихся уголовных преступлений, связанных с компьютерными системами и данными, или для сбора в электронной форме доказательств уголовного преступления.

2 Каждая Сторона должна также принимать такие законодательные и иные меры, которые могут быть необходимы для выполнения обязательств, изложенных в Статьях 27 по 35.

3 Каждая Сторона может, в случае чрезвычайных обстоятельств, сделать запрос об оказании взаимопомощи или соединения с использованием средств ускоренной связи, в том числе по факсу или по электронной почте, при условии, что такие средства обеспечивают соответствующие уровни безопасности и аутентификации (в том числе с использованием средств шифрования, в случае необходимости), с официальным подтверждением, когда это требуется запрашиваемой Стороной. Запрашиваемая Сторона должна принять и ответить на запрос, произведенный любым таким ускоренные средством коммуникации.

4 За исключением случаев, специально предусмотренных в статьях настоящей главы, взаимопомощь должна быть предоставлена с учетом условий, предусмотренных законодательством запрашиваемой Стороны или применимыми договорами о взаимопомощи, включая основания, на которых запрашиваемая Сторона может отказать в сотрудничестве. Запрашиваемая Сторона не должна осуществлять право отказа в оказании взаимопомощи в отношении преступлений, указанных в Статьях 2 по 11 только на том основании, что просьба касается преступления, которое она полагает налоговым правонарушением.

5 В тех случаях, когда в соответствии с положениями настоящей главы запрашиваемой Стороне разрешено оказывать взаимопомощь в зависимости от наличия двойной уголовной ответственности, это условие считается выполненным, независимо от того, свои законы определили соответствующее деяние в данную категорию преступлений или преступление определено с помощью терминологии запрашивающей Стороны, если деяние, лежащее в основе преступления, для которого запрашивается помощь, является уголовным преступлением в соответствии с ее законами.

В рамках расследования киберпреступлений, осуществляемых на национальном уровне, могут быть обнаружены связи с преступлениями, относящимися к другой стране. В случае органов охраны правопорядка, например расследование детской порнографии, они могут найти информацию о педофилах из других стран, которые участвовали в обмене детской порнографией[1543]. Статья 26 устанавливает положения, которые являются необходимыми для органов охраны правопорядка по информированию иностранных органов охраны правопорядка без угрозы для своего собственного расследования[1544].

Статья 26 – Спонтанная информация

1 Любая Сторона может, в рамках своего внутреннего законодательства и без предварительного запроса направить другой Стороне информацию, полученную в рамках своего собственного расследования, если она полагает, что раскрытие такой информации может способствовать получающей информацию Стороне в возбуждении или проведении расследований или разбирательств, касающихся уголовных преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или может привести к просьбе о сотрудничестве с этой Стороной в соответствии с настоящей главой.

2 До предоставления такой информации, предоставляющая Сторона может просить о том, что это носило конфиденциальный характер и использовалось только при соблюдении условий.

[1542] See Explanatory Report to the Convention on Cybercrime, No. 256.

[1543] This information often leads to successful international investigations. For an overview about large scale international investigations related to child pornography see: *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296, page 4, available at: http://www.ecpat.se/upl/files/279.pdf

[1544] Similar instruments can be found in other Council of Europe Convention. For example Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and Article 28 of the Criminal Law Convention on Corruption. The Council of Europe Conventions are available at: http://www.coe.int.

Если принимающая Сторона не может выполнить такую просьбу, она должна уведомить об этом предоставляющую Сторону, которая в таком случае определяет, должна ли в таком случае информация быть предоставлена. Если принимающая Сторона принимает информацию с соблюдением условий, она обязана выполнить их.

Одно из наиболее важных положений Статьи 26 связано с конфиденциальностью информации. В связи с тем, что ряд расследований может быть проведен успешно, если преступник не знает о происходящем расследовании, Статья 26 обеспечивает предоставляющей стороне запроса конфиденциальности в отношении передаваемой информации. Если конфиденциальность не может быть гарантирована, предоставляющая сторона может отказаться от информационного процесса.

6.3.5 Процедуры, связанные с запросами взаимной помощи и отсутствие применимых международных соглашений

Как и Статья 25, Статья 27 основывается на идее о том, что взаимная правовая помощь должна осуществляться на основе применения соответствующих договоров и аналогичных соглашений, а не ссылок только на Конвенцию. Составители Конвенции решили не создавать режим отдельной обязательной взаимной правовой помощи в рамках Конвенции[1545]. Если другие документы уже нашли свое место, Статьи 27 и 28 не имеют отношения к конкретным запросам. Только в тех случаях, когда другие правила не применяются, Статьи 27 и 28 предусматривают ряд механизмов, которые могут быть использованы для осуществления взаимной правовой помощи.

Наиболее важные аспекты, регулируемые Статьей 27, включают:

- обязательства по созданию назначенных контактных центров для запросов на оказание взаимной правовой помощи[1546];
- требование прямой связи между контактными центрами во избежание долгой процедуры[1547]; и,
- создание баз данных со всех контактных центров Генеральным секретарем Совета Европы.

Кроме того, Статья 27 определяет ограничения, относящиеся к запросам на оказание помощи. Сторона Конвенции может отказать в сотрудничестве:

- в случае политических преступлений; и/или,
- если она считает, что сотрудничество может нанести ущерб ее суверенитету, безопасности, общественному порядку или другим жизненно важным интересам.

Составители Конвенции видели необходимость того, чтобы стороны в некоторых случаях отказались от сотрудничества, с одной стороны, а с другой стороны отметили, что стороны должны осуществлять отказ от сотрудничества с осторожностью во избежание противоречий с изложенными ранее принципами[1548]. Поэтому особенно важно определить термин "другие жизненно важные интересы" в узком смысле. Пояснительный доклад к Конвенции о киберпреступности определяет, что это может быть в том случае, если сотрудничество может привести к радикальным трудностям для запрашиваемой стороны[1549]. С точки зрения составителей, проблемы, связанные с неадекватными законами о защите данных, не считаются проблемами, имеющими жизненно важное значение[1550].

6.3.6 Временные меры по взаимной помощи

Статьи 28–33 являются отражением процессуальных документов Конвенции о киберпреступности[1551]. Конвенция о киберпреступности содержит целый ряд процессуальных документов, которые призваны

[1545] See Explanatory Report to the Convention on Cybercrime, No. 262.
[1546] Regarding the 24/7 network points of contact see below: Chapter 6.3.8.
[1547] See Explanatory Report to the Convention on Cybercrime, No. 265: “Initially, direct transmission between such authorities is speedier and more efficient than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to satisfy legal requirements in the requested Party, and that particularly urgent or sensitive requests are dealt with properly.”
[1548] See Explanatory Report to the Convention on Cybercrime, No. 268.
[1549] See Explanatory Report to the Convention on Cybercrime, No. 269. “Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal.”
[1550] See Explanatory Report to the Convention on Cybercrime, No. 269.
[1551] See above: Chapter 6.2.

улучшить расследования в Государствах-Членах[1552]. Что касается принципа национального суверенитета[1553], эти инструменты могут быть использованы только для проведения расследований на национальном уровне[1554]. Если следователи понимают, что доказательства должны быть собраны за пределами их территории, они должны сделать запрос об оказании взаимной правовой помощи. В дополнение к Статье 18, каждый из документов, установленных Статьями 16–21, имеет соответствующее положение в Статьях 28–33, что позволяет органам охраны правопорядка применять процессуальные документы по запросу иностранного органа охраны правопорядка.

Процессуальные документы	Соответствующее положение ML
Статья 16 – Оперативное обеспечение сохранности хранимой компьютерной информации[1555]	Статья 29
Статья 17 – Оперативное обеспечение сохранности и частичное раскрытие данных о трафике[1556]	Статья 30
Статья 18 – Порядок производства[1557]	
Статья 19 – Поиск и извлечение хранимых компьютерных данных[1558]	Статья 31
Статья 20 – Сбор данных о трафике в режиме реального времени[1559]	Статья 33
Статья 21 – Перехват информационного контента[1560]	Статья 34

6.3.7 Трансграничный доступ к данным, сохраненным в памяти компьютера

В дополнение к чистому отражению процедурных положений составители Конвенции обсудили обстоятельства, при которых органы охраны правопорядка могут получить доступ к компьютерным данным, которые не хранятся на их территории и не находятся под контролем какого-либо лица на их территории. Составители Конвенции удалось договориться о двух случаях, когда расследование должно быть проведено одним органом охраны правопорядка без необходимости в запросе об оказании взаимной правовой помощи[1561]. Дальнейшие соглашения невозможны[1562] и даже достигнутое решение еще критикуется государствами – членами Совета Европы[1563].

Эти два случая, когда органы охраны правопорядка могут получить доступ к данным, хранящимся вне их территории, связаны с:

- общедоступной информацией; и/или
- доступ с согласия управляющего лица.

[1552] The most important instruments established by the Convention on Cybercrime are: Expedited preservation of stored computer data (Art. 16), Expedited preservation and partial disclosure of traffic data (Art. 17), Production order (Art. 18), Search and seizure of stored computer data (Art. 19), Real-time collection of traffic data (Art. 20), Interception of content data (Art. 21).
[1553] National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.
[1554] An exemption is Art. 32 Convention on Cybercrime – See below. Regarding the concerns related to this instrument see: Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2: " […]Russian Federation (had a positive approach towards the Convention but further consideration would have to be given to Article 32b in particular in the light of experience gained from the use of this Article).
[1555] See above: Chapter 6.2.4.
[1556] See above: Chapter 6.2.4.
[1557] See above: Chapter 6.2.7.
[1558] See above: Chapter 6.2.6.
[1559] See above: Chapter 6.2.9.
[1560] See above: Chapter 6.2.410.
[1561] See Explanatory Report to the Convention on Cybercrime, No. 293.
[1562] "The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules." See Explanatory Report to the Convention on Cybercrime, No. 293.
[1563] See below in this chapter.

Статья 32 – Трансграничный доступ к данным, хранящимся в памяти компьютера, с соответствующего согласия или к общедоступным данным

Сторона может без согласия другой Стороны:

a) получать доступ к общедоступным (открытому источнику) данным, хранящимся в памяти компьютера, независимо от их географического местоположения; или

b) получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их, если эта Сторона имеет законное и добровольное согласие лица, которое имеет законные полномочия раскрывать эти данные этой Стороне через такую компьютерную систему.

Другие ситуации не подпадают под действие Статьи 32, но также не исключаются[1564].

Статья 32 отмечает, что, если соответствующие данные являются общедоступными, иностранные органы охраны правопорядка имеют право доступа к этой информации. Примером общедоступной информации является информация на веб-сайтах без контроля доступа, например паролей. Если следователям не будет, в отличие от любого другого пользователя, разрешен доступ к этим веб-сайтам, это может серьезно затруднить их работу. Таким образом, эта первая ситуация, рассмотренная в Статье. 32, широко распространена.

Второй ситуацией, при которой органы охраны правопорядка могут получить доступ к данным, хранящимся на компьютере за пределами их территории, является ситуация, когда следователи получили законное и добровольное согласие лица, которое имеет законные полномочия раскрывать данные. Это разрешение подверглось суровой критике[1565]. Существуют веские аргументы против такого регулирования. Наиболее важным из них является тот факт, что созданием второго случая составители Конвенции нарушают догматичную структуру режима взаимной правовой помощи. В Статье 18 составители Конвенции позволили расследование в порядке представления данных. Этот документ не может быть применен при проведении международных расследований, поскольку соответствующее положение в главе 3 Конвенции отсутствует. Вместо отказа от догматического структуры, позволяющего иностранным следователям вступать в непосредственный контакт с лицом, осуществляющим контроль над данными, и просить о представлении данных, авторы могли бы просто ввести соответствующие положения Главы 3 Конвенции[1566].

6.3.8 Сеть связи 24/7

Расследования киберпреступлений часто требуют немедленной реакции[1567]. Как указывалось выше, это особенно актуально, когда речь идет о данных о трафике, которые необходимы для идентификации подозреваемых, поскольку они часто удаляются в течение довольно короткого периода времени[1568]. Для увеличения скорости международных расследований Европейская конвенция о киберпреступности подчеркивает важность создания условий для усиленного использования средств коммуникации в Статье 25. В целях дальнейшего повышения эффективности запросов об оказании взаимопомощи составители конвенции обязали стороны назначить контактные центры для запросов об оказании взаимопомощи, которые доступны без каких-либо временных ограничений[1569]. Составители Конвенции подчеркнули, что создание

[1564] See Explanatory Report to the Convention on Cybercrime, No. 293.
[1565] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.
[1566] In this context it is necessary to point out a difference between Art. 32 and Art. 18. Unlike Art. 18 Art. 32 does not enable the foreign law enforcement agency to order the submission of the relevant data. It can only seek for permission.
[1567] The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."
[1568] See above: Chapter 6.2.4.
[1569] The availability 24 hours a day and 7 days a week is especially important with regard to international dimension of Cybercrime as requests can potentially come from any time zone in the world. Regarding the international dimension of Cybercrime and the related challenges see above: Chapter 3.2.6.

контактных центров является одним из наиболее важных документов, предусмотренных Конвенцией о киберпреступности[1570].

> ***Статья 35 – Сеть 24/7***
>
> *1 Каждая Сторона назначает контактный центр, работающий 24 часа в сутки семь дней в неделю, для обеспечения оказания неотложной помощи в целях расследований или судебных разбирательств уголовных преступлений, относящихся к компьютерным системам и данным, или в целях сбора доказательств в электронной форме по уголовным преступлениям. Такая помощь должна включать содействие или, если это допускается внутригосударственным правом или практикой, непосредственное применение следующих мер:*
>
> *a) оказание технической консультативной помощи;*
>
> *b) обеспечение сохранности данных в соответствии со Статьями 29 и 30;*
>
> *c) сбор доказательств, предоставление законной информации и установление нахождения подозреваемых.*
>
> *2a) Контактный центр одной Стороны должен располагать возможностями для оперативного обмена сообщениями с контактным центром другой Стороны.*
>
> *b) Если контактный центр, назначенный одной из Сторон, не входит в состав органа или органов этой Стороны, уполномоченных оказывать взаимопомощь или экстрадицию, этот контактный центр принимает меры для оперативной координации своей деятельности с деятельностью такого органа или органов.*
>
> *3) Каждая Сторона должна принимать меры для предоставления квалифицированного персонала и оборудования с целью облегчить функционирование такой сети.*

Идея Сети 24/7 основана на существующей сети для круглосуточных контактов по международной преступности в сфере высоких технологий Группы восьми[1571]. При создании контактных центров Сети 24/7 составители Конвенции сосредоточились на решении проблем борьбы с киберпреступностью, особенно тех, которые имеют отношение к процессам скорости обмена данными[1572] и имеют международный масштаб[1573]. Стороны Конвенции обязаны создать такие контактные центры и обеспечить возможность их немедленного реагирования, как и основных услуг. Как указывается в подпункте 3 Статьи 34 Конвенции о киберпреступности, это включает подготовку и оснащение персонала.

Относительно процесса создания контактного центра и в особенности основополагающих принципов данной структуры, Конвенция позволяет максимальную гибкость государствам-членам. Конвенция не требует создания нового органа и не определяет, какие из существующих органов могут или должны быть наделены полномочиями контактного центра. Составители Конвенции также указывают на тот факт, что точки Сети 24/7 предназначены для оказания как технической, так и юридической помощи, что приведет к различным вариантам возможных решений ее осуществления.

Применительно к расследованию киберпреступлений установка контактных центров имеет две основные функции. Они включают в себя:

[1570] See Explanatory Report to the Convention on Cybercrime, No. 298.

[1571] Regarding the activities of the G8 in the fight against Cybercrime see above: Chapter 5.1.1 . For more information on the 24/7 Network see: See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol 9, page 484, available at: http://www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.pdf.

[1572] See above: Chapter 3.2.10.

[1573] See above: Chapter 3.2.6.

- ускорения связи в результате предоставления единого контактного центра; и
- ускорения расследований при предоставлении контактному центру функций вывода основных прав расследования.

Сочетание двух функций является потенциалом для приближения скорости международных расследований к уровню, достигаемому в рамках национальных расследований.

Статья 32 Конвенции о киберпреступности определяет минимально необходимые показатели узла сети. Помимо технической помощи и предоставления правовой информации, основные задачи контактного пункта включают:

- сохранение данных;
- сбор доказательств; и,
- определение местоположения подозреваемых.

В этом контексте еще раз важно подчеркнуть, что Конвенция не определяет, какой орган должен отвечать за эксплуатацию контактного центра 24/7. Если контактным центром управляет один орган, обладающий компетенцией в целях сохранения данных[1574], а иностранный контактный центр запросил такие данные, эта мера может быть немедленно выполнена местным контактным центром. Если контактный центр находится в ведении органа, который не является самостоятельно компетентным в целях сохранения данных, важно чтобы контактный центр имеет возможность сразу обратиться в компетентные органы для обеспечения того, чтобы немедленного осуществления этой меры[1575].

На 2-м совещании комитета Конвенции о киберпреступности было четко указано, что участие в работе сети связи 24/7 не требует подписания и ратификации Конвенции[1576].

6.3.9 Международное сотрудничество в проекте Стэнфордской конвенции

Составители Проекта Стэнфордской конвенции[1577] признали важность международного аспекта киберпреступности и связанные с этим проблемы. В целях решения этих проблем они включили конкретные положения, которые связаны с международным сотрудничеством. Положения охватывают следующие темы:

- Статья 6 – Взаимная правовая помощь,
- Статья 7 – Экстрадиция,
- Статья 8 – Преследование,
- Статья 9 – Предварительные средства судебной защиты,
- Статья 10 – Права обвиняемого,
- Статья 11 – Сотрудничество в правоохранительной сфере.

Такой подход показывает ряд сходств с подходом, принятым в Конвенции о киберпреступности. Основное различие заключается в том, что правила, предусмотренные Конвенцией о киберпреступности более строгие, более сложные и более точно определены по сравнению с Проектом Стэндфордской конвенции. Как отметили составители Проекта Стэнфордской конвенции, подход к Конвенции о киберпреступности является более практичным и, следовательно, имеет некоторые явные преимущества с точки зрения фактического

[1574] Regarding the question which authorities should be authorised to order the preservation of data see above: Chapter 6.2.4.
[1575] Explanatory Report to the Convention on Cybercrime, No. 301.
[1576] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).
[1577] The Stanford Draft International Convention (CISAC) was developed as a follow up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 et seq., available at: http://media.hoover.org/documents/0817999825_249.pdf; For more information see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

применения[1578]. Составители Проекта Стэнфордской конвенции решили придерживаться другого подхода, как они предсказывали, что внедрение новых технологий может привести к некоторым трудностям. В результате они лишь определили некоторые общие инструкции, не определяя их в дальнейшем[1579].

6.4 Ответственность поставщиков услуг интернета

6.4.1 Введение

Совершение киберпреступления автоматически вовлекает ряд людей и предприятий, даже если преступник действовал один. Из-за структуры сети интернет для передачи простой электронной почты требуется обслуживание нескольких поставщиков[1580]. В дополнение к электронной почте передающий поставщик привлекает поставщиков услуг доступа, а также маршрутизаторы, которые передают электронную почту получателю. Относительно загрузки фильмов, содержащую детскую порнографию, ситуация аналогична. Процесс загрузки вовлекает поставщика информации, который загружал картинки, например на веб-сайт поставщика услуг хостинга, который предоставлял место для хранения информации на веб-сайте, маршрутизаторы, которые направляли файлы пользователю и, наконец, поставщика услуг доступа, предоставляющего пользователю доступ в интернет.

Из-за этой причастности разных сторон, поставщики услуг интернета с тех пор оказались в центре внимания уголовных расследований, направленных против преступников, использующих услуги поставщиков с целью совершения преступления[1581]. Одной из главных причин такого развития событий послужил тот факт, что даже если преступник действует из-за рубежа, поставщики, находящиеся в пределах национальных границ являются подходящим объектом для уголовных расследований, при этом не нарушается принцип государственного суверенитета[1582].

Тот факт, что киберпреступление, с одной стороны, не может быть совершено без привлечения поставщиков услуг, а с другой стороны, что зачастую поставщики не имеют возможности предупреждения этих преступлений, привели к вопросу, нужно ли ограничивать ответственность поставщиков услуг интернета[1583]. Ответ на данный вопрос очень важен для экономического развития инфраструктуры ИКТ. Поставщики будут предоставлять только свои услуги, если они не смогут избежать уголовной ответственности в режиме обычной работы. Кроме того, к данному вопросу имеют большой интерес и органы охраны правопорядка. Работа органов охраны правопорядка часто зависит от сотрудничества, в том числе и поставщиков услуг интернета. Это вызывает некое беспокойство, как ограниченная ответственность поставщиков услуг интернета за действия, совершенные их пользователями, может повлиять на сотрудничество с поставщиками услуг интернета и поддержку расследований киберпреступлений, а также фактическое предупреждение преступления.

6.4.2 Подход Соединенных Штатов

Существуют различные подходы, позволяющие сбалансировать, с одной стороны, необходимость активного участия поставщиков в расследованиях и предельными рисками уголовной ответственности за действия третьих лиц, с другой стороны[1584]. Пример законодательного подхода можно найти в 17 U.S.C. п.п. 517 a) и b).

[1578] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1579] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: http://www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1580] Regarding the network architecture and the consequences with regard to the involvement of service providers see: *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003, available at: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

[1581] See in this context: Sellers, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: http://www.okjolt.org/pdf/2004okjoltrev8a.pdf.

[1582] National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: http://www.law.uga.edu/intl/roth.pdf.

[1583] For an introduction into the discussion see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 et seq. - available at http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf

[1584] In the decision Recording Industry Association Of America v. Charter Communications, Inc. the United States Court of Appeals for the eighth circuit described (by referring to House Report No. 105-551(II) at 23 (1998)) the function of the United States DMCA by pointing out the balance. In the opinion of the court the DMCA has “two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights.”

§ 512 Ограничения ответственности, связанные с материалами, доступными онлайн

a) Связь по транзитной цифровой сети

Поставщик услуги не несет ответственности за денежное возмещение или, за исключением случаев, предусмотренных в подпункте (j), за назначенное пособие или другие судебные взыскания, за нарушение авторских прав по причине передачи, выполненной поставщиком, маршрутизации или предоставлении соединения, за передачу через систему или сеть материалов, контролируемых или эксплуатируемых им или поставщиком услуги, или за промежуточное или временное хранение этого материала в ходе такой передачи, маршрутизации или предоставление соединений, если

1) передача материала произошла по инициативе или указанию лица, не являющимся поставщиком услуги;

2) передача, маршрутизация, предоставление соединений или хранение осуществляется поставщиком услуги по средству автоматического технического процесса без сортировки материала;

3) поставщик услуги не выбирает получателей материала, за исключением случаев автоматического ответа на просьбу другого лица;

4) поставщиком услуги не сделана ни одна копия материала в ходе такого промежуточного или временного хранения, поддерживаемого системой или сетью в таком виде, как обычное открытое хранение для любых других ожидающих получателей, или не сделана ни одна копия материала в системе или сети в виде обычного открытого доступа ожидающих получателей за долгий период, когда допустима необходимость для передачи, маршрутизации или предоставления соединений; и

5) материал передался через систему или сеть без изменения его содержания.

b) Система кэширования

1) Ограничение ответственности. Поставщик услуги не несет ответственности за денежное возмещение или, за исключением случаев, предусмотренных в подпункте (j), за назначенное пособие или другие судебные взыскания, за нарушение авторских прав по причине передачи, выполненной поставщиком, маршрутизации или предоставлении соединения, за передачу через систему или сеть материалов, контролируемых или эксплуатируемых им или поставщиком услуги, в случае когда

A) материал доступен онлайн другому лицу, не являющемуся поставщиком услуги;

B) материал передан от лица, указанного в подпункте A) в направлении другого лица, через систему или сеть лицу, отличному от лица, указанного в подпункте A); и

C) хранение осуществляется посредством автоматического выполнения технического процесса с целью создания материала доступного для пользователей системы или сети, которые после того, как это материал будет передан, в соответствии с описанием подпараграфа B), запросит доступ к материалу от лица, описанного в подпараграфе A), если выполняются условия, установленные в параграфе 2).

Данное положение основано на DMCA (Закон о защите авторских прав в цифровую эпоху), который был подписан в 1998 году[1585]. Благодаря созданию режима "безопасной гавани", закон DMCA исключает ответственность поставщиков определенных услуг за нарушение авторских прав третьими лицами[1586]. В его

[1585] Regarding the History of the DMCA and the Pre-DMCA case law in the United States see: *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: http://www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Salow*, Liability Immunity for Internet Service Providers – How is it working?, Journal of Technology Law and Policy, Vol. 6, Issue 1, 2001, available at: http://grove.ufl.edu/~techlaw/vol6/issue1/pearlman.html.

[1586] Regarding the DMCA impact on the liability of Internet Service Provider see: *Unni*, Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001 - available at: http://www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 et seqq., available at: http://www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 et seq. , available at http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; Schwartz, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology

содержании, прежде всего, важно выдвинуть на первый план тот факт, что не на всех поставщиков распространяется данное ограничение[1587]. Ограниченная ответственность распространяется только на поставщиков услуг[1588] и поставщиков услуг кэширования[1589]. Кроме того, важно отметить, что ответственность связана с определенными требованиями. Что касается поставщиков услуг, то требования такие:

- передача материала произошла по инициативе или указанию лица, не являющимся поставщиком услуги;
- передача произошла при помощи автоматического технического процесса без отбора материала поставщиком услуги;
- поставщик услуги не выбирает получателей материала;
- ни одна копия материала, сделанного поставщиком услуги в ходе такого промежуточного или временного хранения, не сохраняется в системе или сети таким образом, какой обычно доступен ни для кого, кроме ожидающих получателей.

Другой пример ограниченной ответственности поставщиков услуг интернета можно найти в 47 U.S.C. § 230 c), который основывается на Акте о соблюдении приличий в СМИ[1590]:

> ***§ 230 Защита с целью блокировки и проверка оскорбительного материала***
>
> *c) Защита для выполнения блокировки "Добрых Самаритян" и проверка оскорбительного материала*
>
> *1) Воздействие на издателя или поставщика*
>
> *Ни одного поставщика или пользователя интерактивными компьютерными услугами нельзя рассматривать как издателя или поставщика любой информации, предоставленной другим поставщиком, имеющим информацию.*
>
> *2) Гражданская ответственность*
>
> *Ни один поставщик или пользователь интерактивных компьютерных услуг не должен нести ответственность в результате*
>
> *A) любого действия, добровольно ограничивающего доступ к имеющемуся материалу, который поставщик или пользователь считают непристойным, развратным, похотливым, грязным, чрезмерно жестоким, оскорбительным, или по другим причинам, независимо от того, защищены эти материалы конституционно или нет; или B) любого предпринятого действия, дающего право или предоставляющего поставщику услуг информационного контента или другим лица технических средств ограничения доступа к материалу, описанному в параграфе 1).*

Оба подхода, изложенных в 17 U.S.C. § 517 a), также как и 47 U.S.C. § 230 c), вместе обращают внимание на ответственность в отношении специальных групп поставщиков и специальных областей закона. Поэтому оставшаяся часть главы даст краткий обзор законодательного подхода от Директивы Европейского союза по электронной торговле.

Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html.

[1587] Regarding the application of the DMCA to Search Engines see: *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: http://www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

[1588] 17 U.S.C. § 512(a)

[1589] 17 U.S.C. § 512(b)

[1590] Regarding the Communication Decency Act see: *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 et seqq., available at: http://www.smu.edu/csr/articles/2005/Fall/SMC103.pdf;

6.4.3 Директива Европейского союза по электронной торговле

Примером законодательного подхода, чтобы регулировать ответственность поставщиков услуг интернета, является Директива Европейского союза по электронной торговле[1591]. Столкнувшись с проблемами, касающимися международного использования интернета, создатели Директивы разработали правовые стандарты, которые обеспечивают поставщику законодательную основу для комплексного развития информационного общества, при этом поддерживая комплексное экономическое развитие, так же как и работу органов охраны правопорядка[1592]. Регулирование относительно ответственности основано на принципе переходящей надежности.

Директива содержит ряд положений, которые ограничивают ответственность некоторых поставщиков[1593]. Ограничения связаны с различными категориями предоставляемых поставщиком услуг[1594]. Во всех других случаях ответственность не обязательно исключена, и, если она ограничена другими положениями, человек полностью ответственен. Мотивация Директивы состоит в ограничении ответственности в тех случаях, когда поставщик имеет лишь ограниченные возможности предотвращения преступления. Причины ограниченных возможностей могут быть технического характера. Маршрутизаторы, например, без существенной потери скорости не способны отфильтровывать проходящие через них данные и едва ли способны предотвратить процессы обмена данными. Поставщики услуг хостинга могут удалить данные, если они извещены о преступной деятельности. Однако как и маршрутизаторы, крупные поставщики услуг хостинга не могут контролировать все данные, хранящиеся на их серверах.

Так как не всегда удается контролировать активность преступной деятельности, ответственность поставщиков услуг хостинга и поставщиков услуг доступа отличается. Относительно того, что необходимо учесть фактическую ответственность, баланс Директивы основан на текущих технических стандартах. На данный момент нет доступных инструментов, которые могли бы автоматически обнаруживать неизвестные порнографические изображения. Если в этой области продолжится техническое развитие, в будущем необходимо будет оценить техническую возможность поставщиков, откорректировать систему.

6.4.4 Ответственность поставщиков услуг доступа в интернет (Директива Европейского союза)

Статьи 12–15 определяют степень ограничения ответственности различных поставщиков. На основании Статьи 12, ответственность поставщиков доступа и операторов, осуществляющих маршрутизацию, полностью исключается, если они соответствуют трем условиям, изложенным в Статье 12. Как следствие, поставщик услуг доступа в целом не несет ответственности за уголовные преступления, совершенные его пользователями. Такое полное освобождение от ответственности не освобождает поставщика от обязанности по предотвращению дальнейших преступлений по распоряжению суда или административного органа[1595].

> ***Статья 12 – "Чистый канал"***
>
> *1 В случае предоставления услуги информационного общества, состоящей из передачи по сети связи информации, предоставленной получателем услуги или предоставление доступа к сети связи, государства-члены должны гарантировать, что поставщик услуги не несет ответственности за переданную информацию, при условии что поставщик:*
>
> *a) не определил передачу;*
>
> *b) не выбивал получателя передачи; и*
>
> *c) не выбирал или изменял информацию, содержащуюся в передаче.*

[1591] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178 , 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive) see: Pappas, Comparative U.S. & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol 31, 2003, pae 325 et seqq., available at: http://www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf

[1592] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

[1593] Art. 12 – Art. 15 EU E-Commerce Directive.

[1594] With the number of different services covered the E-Commerce Directive aims for a broader regulation than 17 U.S.C. § 517(a). Regarding 17 U.S.C. § 517(a) see above:

[1595] See Art. 12 paragraph 3 E-Commerce Directive.

2 Процессы передачи и предоставление доступа, упомянутые в пункте 1, включают автоматическое, промежуточное и временное хранение информации, переданной таким образом, чтобы занять место при передаче в сети связи, и эта информация не сохранилась течение некоторого периода, который был дольше, чем время, разумно требуемое для передачи.

3 Настоящая статья не влияет на возможности для суда или административного органа в соответствии с законодательными системами государств-членов, требующих, чтобы поставщик услуги прекратил или предотвратил нарушение.

Этот подход сопоставим с 17 U.S.C. § 517 a)[1596]. Оба положения нацелены на определение ответственности поставщиков услуг и определяют связь ограниченной ответственности с аналогичными требованиями. Главным отличием фактически является то, что приложение Статьи 12 Директивы Европейского союза по электронной торговле, не ограничивает нарушения авторских прав, но исключает ответственность в отношении какого-либо преступления.

6.4.5 Ответственность за кэширование (Директива Европейского союза)

Термин "кэширование", используемый в данном контексте, описывает хранение популярных веб-сайтов на местных носителях таким образом, чтобы уменьшить пропускную способность и сделать доступ к данным более эффективным[1597]. Одним из методов, используемых для снижения пропускной способности является установка прокси-серверов[1598]. В этом случае прокси-сервер может обслуживаться без контактирования с установленным сервером (доменное имя введено пользователем) путем извлечения сохраненного контекста в местном носителе из предыдущего запроса. Составители Директивы признали экономическую важность кэширования и решили исключить ответственность за автоматическое временное хранение, если поставщик соблюдает условия, определенные Статьей 13. Одним из условий является то, что поставщик соблюдает повсеместно признанные стандарты относительно обновления информации.

Статья 13 – "Кэширование"

1 В случае предоставления услуги информационного общества, состоящей из передачи по сети связи информации, предоставленной получателем услуги, государства-члены должны гарантировать, что поставщик услуги не несет ответственности за автоматическое, промежуточное и временное хранение такой информации, представленной для единственной цели, сделать более эффективной дальнейшую передачу информации к получателям услуги по его запросу, при условии что:

a) поставщик не изменяет информацию;

b) поставщик соблюдает условия доступа к информации;

c) поставщик соблюдает правила обновления информации, установленные в рамках повсеместного признания и использования в промышленности;

d) провайдер не нарушает законное применение технологии, которая признана повсеместно и используется в промышленности, обновляет данные в используемой информации; и

e) поставщик действует оперативно тогда, когда он получил фактические данные о том, что к информации, которая хранится у него, необходимо удалить или запретить доступ, что

[1596] The provision was implemented by the DMCA (Digital Millennium Copyright Act). Regarding the DMCA impact on the liability of Internet Service Provider see: *Unni*, Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001 - available at: http://www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 et seqq., available at: http://www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 et seq. - available at http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf

[1597] With regard to the traditional caching as well as active caching see: Naumenko, Benefits of Active Caching in the WWW, available at: http://lcawww.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

[1598] For more information on Proxy Servers see: *Luotonen*, Web Proxy Servers, 1997.

информация была удалена из сети, или доступ к ней поврежден, или что суд или административный орган предписал ее удаление или перемещение.

2 Настоящая статья не влияет на возможности для суда или административного органа в соответствии с законодательными системами государств-членов, требующих, чтобы поставщик услуги прекратил или предотвратил нарушение.

Статья 13 Директивы Европейского союза по электронной торговле является другим примером сходства между безапелляционной структурой Соединенных Штатов и европейского подхода. Подход Европейского союза сопоставим с 17 U.S.C. § 517 b)[1599]. Оба положения нацелены на определение ответственности поставщиков услуг кэширования и определяют связь ограниченной ответственности с аналогичными требованиями. Что касается ответственности поставщиков услуг[1600], главным отличием фактически является то, что приложение Статьи 13 Директивы Европейского союза по электронной торговле не ограничивает нарушение авторских прав, но исключает ответственность в отношении какого-либо преступления.

6.4.6 Ответственность поставщиков услуг хостинга (Директива Европейского союза)

В особенности в связи с незаконным содержанием поставщик услуг хостинга выполняет важную функцию при совершении преступления. Преступники, которые создают незаконное содержание, доступное онлайн, в основном не хранят его на своих серверах. Большинство веб-сайтов хранятся на серверах, которые сделаны доступными поставщиками услуг хостинга. Каждый, кто захочет запустить веб-страницу может арендовать емкость у поставщика услуг хостинга и хранить там веб-сайт. Некоторые поставщики даже часто сами руководят организацией загрузки свободного веб-пространства[1601].

Выявление незаконного содержания является вызовом для провайдера услуг хостинга. Ручной поиск незаконного содержания на большом количестве веб-сайтов будет невозможен, особенно для популярных поставщиков со множеством веб-сайтов.

В результате составители Директивы решили ограничить ответственность поставщиков услуг хостинга. Однако в отличие от поставщика услуг доступа, ответственность поставщика услуг хостинга не исключается. До тех пор пока поставщик услуг хостинга не имеет реальных сведений о незаконной деятельности или незаконном содержании, хранящимся на его сервере, то он не несет ответственности. Предположение, что незаконное содержание могло быть сохранено на серверах, здесь не считается эквивалентным реальной осведомленности о проблеме. Если поставщик получает конкретную информацию о незаконной деятельности или незаконном содержании, то он может избежать ответственности только в случае, если он немедленно удалит незаконную информацию[1602]. Неспособность немедленно реагировать приведет к ответственности поставщика услуг хостинга[1603].

Статья 14 – Хостинг

1 В случае предоставления услуги информационного общества, состоящей из хранения информации, предоставленной получателем услуги, государства-члены должны гарантировать, что, поставщик услуги не несет ответственности за информацию, хранящуюся на сервере, при условии что:

а) поставщик фактически не осведомлен о незаконной деятельности или информации и, что касается жалоб на опасность, ему не известны факты или условия, какая имеется незаконная информация, или какие совершаются незаконные действия; или

[1599] The provision was implemented by the DMCA (Digital Millennium Copyright Act). Regarding the DMCA impact on the liability of Internet Service Provider see: *Unni*, Internet Service Provider's Liability for Copyright Infringement - How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001 - available at: http://www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 et seqq. , available at: http://www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 et seq., available at http://www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf

[1600] See above: Chapter 6.4.4.

[1601] Regarding the impact of free webspace on criminal investigations see: Evers, Blogging sites harbouring cybercriminals, CNET News, 26.07.2005, available at: http://news.zdnet.co.uk/security/0,1000000189,39210633,00.htm.

[1602] This procedure is called "notice and takedown"

[1603] The hosting provider is quite often in a difficult situation. On the one hand side he needs to react immediately to avoid liability – on the other hand side he has certain obligations with regard to his customers. If he removes legal information that was just on first sight illegal, this could lead to claims for indemnity.

b) поставщик после получения таких знаний или сведений действует быстро с целью удалить или запретить доступ к информации.

2 Пункт 1 не должен применяться, когда получатель услуги действовал под руководством или контролем поставщика.

3 Настоящая статья не влияет на возможности для суда или административного органа в соответствии с законодательными системами государств-членов, требующих, чтобы поставщик услуг закончил или предотвратил нарушение, при этом это не затрагивает возможность для государств-членов установления процедур, управляющих перемещением или запрещением доступа к информации.

Статья 14 применяется не только для поставщика, который ограничивает свои услуги арендой технической инфраструктуры для хранения данных. Популярные услуги интернета, являются актуальной платформой предлагаемым услугам хостинга[1604].

6.4.7 Исключение обязательств по мониторингу (Директива Европейского союза)

Перед тем, как Директива была внедрена, она имела неопределенность в некоторых государствах-членах, в случае если поставщики подвергаются судебному преследованию за нарушение обязательства по мониторингу деятельности пользователей. Помимо возможных конфликтов с правилами защиты данных и защите тайны электросвязи, такое обязательство будет особенно вызывать трудности для поставщиков услуг хостинга, которые хранят тысячи веб-сайтов. Чтобы избежать таких конфликтов, Директива исключает общее обязательство по мониторингу передаваемой или хранимой информации.

Статья 15 – Нет основных обязательств по мониторингу

1 Государства-члены не будут навязывать поставщикам общее обязательство, при предоставлении услуг, предусмотренных Статьями 12, 13 и 14, чтобы контролировать информацию, которую они передают или хранят, ни общее обязательство активно искать факты или обстоятельства, свидетельствующие о незаконной деятельности.

2 Государства-члены могут устанавливать обязательства поставщикам услуг информационного общества услуг незамедлительно информировать компетентные государственные органы о якобы незаконных предпринятых действиях или информации, предоставленной получателям их услуги, или обязательства сообщать в компетентные органы, по их просьбе, информацию, позволяющую идентифицировать получателей их услуг, с которыми они хранят соглашения.

6.4.8 Ответственность за гиперссылки (ECC Австрии)

Гиперссылки играют важную роль в интернете. Они позволяют поставщику гиперссылки направить пользователя конкретной информации, доступной онлайн. Вместо того чтобы просто предлагать технические подробности о том, как информация может быть доступна (например, путем предоставления доменного имени сайта, где информация предоставляется), пользователь может напрямую получить доступ к информации, нажав на активную ссылку. Гиперссылка дает команду для веб-браузера открыть установленный адрес интернет.

В рамках составленной Директивы Европейского союза интенсивно обсуждалась необходимость создания правил по гиперссылкам[1605]. Составители решили не обязывать государства-члены согласовывать свои законы, касающиеся ответственности за гиперссылки. Вместо этого они осуществили повторное обсуждение процедуры для обеспечения того, чтобы была принята во внимание необходимость в предложениях, касающихся ответственности поставщиков гиперссылок и местоположения инструментальных услуг[1606]. До

[1604] By enabling their customers to offer products they provide the necessary storage capacity for the required information.

[1605] *Spindler*, Multimedia und Recht 1999, page 204.

[1606] Art. 21 – Re-examination

1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.
2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, 'notice and take down' procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.

тех пор пока положение об ответственности за гиперссылки не будет в будущем изменено, Государства-Члены могут свободно разрабатывать национальные решения[1607]. Некоторые страны Европейского союза решили рассмотреть ответственность поставщиков за гиперссылки в специальном положении[1608]. Эти страны основывали ответственность поставщиков гиперссылок на тех же принципах, что предусматривает директива в отношении ответственности поставщиков услуг хостинга[1609]. Этот подход является логическим следствием аналогичной ситуации поставщика услуг хостинга и поставщика гиперссылок. В обоих случаях поставщики контролируют незаконное содержание или, по крайней мере, ссылку на это содержание.

Пример Раздел 17 ECC Австрии[1610]:

> ***Раздел 17 ECC (Австрия) – Ответственность за гиперссылки***
>
> *1) Поставщик, обеспечивающий доступ к информации, предоставленной третьим лицом посредством предоставления электронной связи, не несет ответственности за информацию если он*
>
> *1 не имеет фактических данных о незаконной деятельности или информации, и в случае иска о возмещении ущерба за это ничего не известно о фактах или обстоятельствах, из которых следовало бы, что поставщик услуги совершал действия или предоставлял информацию незаконно; или*
>
> *2 после получения таких данных или сведений, смог быстро прекратить электронную связь.*

6.4.9 Ответственность поисковых машин

Поставщики поисковых машин предлагают услуги поиска по нахождению интересующих документов, обладающих определенными критериями. Поисковая машина будет искать соответствующие документы, которые соответствуют критериям, введенным пользователем. Поисковые машины играют важную роль в успешном развитии интернета. Содержание, сделанное доступным на веб-сайте, но не перечисленное в индексе поисковой машине, могут быть доступно только в том случае, если лицо, желающее получить доступ к нему, знает полный URL-адрес. *Introna/Nissenbaum* указывает на то, что "без особого преувеличения можно сказать, что существование заключается в том, чтобы быть индексированным в поисковых машинах"[1611].

Как и в случае с гиперссылками Директива Европейского союза не содержит стандартов, которые определяют ответственность операторов поисковых машин. Таким образом, некоторые страны Европейского союза приняли решение рассмотреть ответственность поставщиков поисковых машин в специальном положении[1612]. В отличие от гиперссылок регулирование не во всех странах основывается на одних и тех же принципах[1613]. Испания[1614] и Португалия основываются на своих правилах, касающихся ответственности

[1607] *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.
[1608] Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.
[1609] See report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.
[1610] § 17 - Ausschluss der Verantwortlichkeit bei Links
(1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Informationen nicht verantwortlich, sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder, sobald er diese Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.
[1611] *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, Page 5. Available at: http://www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf
[1612] Austria, Spain and Portugal. See report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.
[1613] See report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.
[1614] Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) - Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a conteni-dos o instrumentos de búsqueda (Spain)
1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente. Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere la letra a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.
2. La exención de responsabilidad establecida en el apartado primero no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

операторов поисковых машин в соответствии со Статьей 14 Директивы, в то время как Австрия [1615] основывается на ограничении ответственности в соответствии со Статьей 12.

> ***Раздел 14 ECC (Австрия) – Ответственность операторов поисковых машин***
>
> *1) Поставщик, который предоставляет поисковую машину или другие электронные средства для поиска информации, предоставленную третьим лицом, не несет ответственности, при условии что поставщик:*
>
> *1 не определил передачу;*
>
> *2 не выбирал получателя передачи; и*
>
> *3 не выбирал или изменял информацию, содержащуюся в передаче.*

7 ПРАВОВЫЕ СПРАВОЧНЫЕ ДОКУМЕНТЫ

Конвенция о киберпреступности[1616],

Типовой закон Содружества о компьютерах и компьютерных преступлениях[1617],

Проект Стэнфордской Конвенции[1618].

[1615] Ausschluss der Verantwortlichkeit bei Suchmaschinen
§ 14. (1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er
1. die Übermittlung der abgefragten Informationen nicht veranlasst,
2. den Empfänger der abgefragten Informationen nicht auswählt und
3. die abgefragten Informationen weder auswählt noch verändert.
(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.
[1616] Council of Europe Convention on Cybercrime, available at: http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm
[1617] Commonwealth Model Law on Computer and Computer Related Crime, available at: http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf
[1618] Draft Stanford Convention, available at: http://www.stanford.edu/~gwilson/Transnatl.Dimension.Cyber.Crime.2001.p.249.pdf

Отпечатано в Швейцарии
Женева, 2009 г.