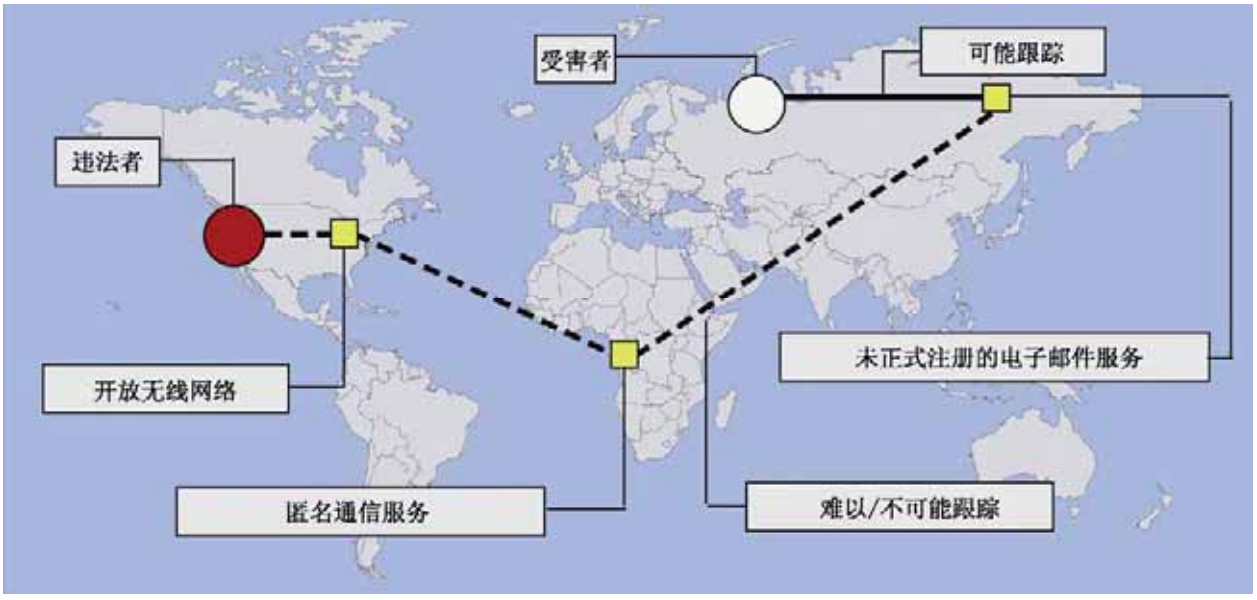
国　　际　　电　　信　　联　　盟



了解网络犯罪：针对发展中国家的指南

国际电联电信发展部门
政策和战略部
信息通信技术应用与网络安全处

2009 年 4 月草案

欲了解更多信息，请联系

ITU-D 信息通信技术应用与网络安全处：cybmail@itu.int

国际电信联盟

致谢

应国际电联发展部门（ITU-D）信息通信技术应用与网络安全处委托提交本报告。

《了解网络犯罪：一个针对发展中国家的指南》由 Marco Gercke 博士负责完成。作者希望感谢国际电联电信发展部门工作团队给予的支持，并感谢 Gunhild Scheer 的热烈讨论。

国际电联出版物《了解网络犯罪：一个针对发展中国家的指南》可在以下网址找到：

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

本文档版式已按正反面打印要求处理。本文档已经发布，但未做正式编辑。

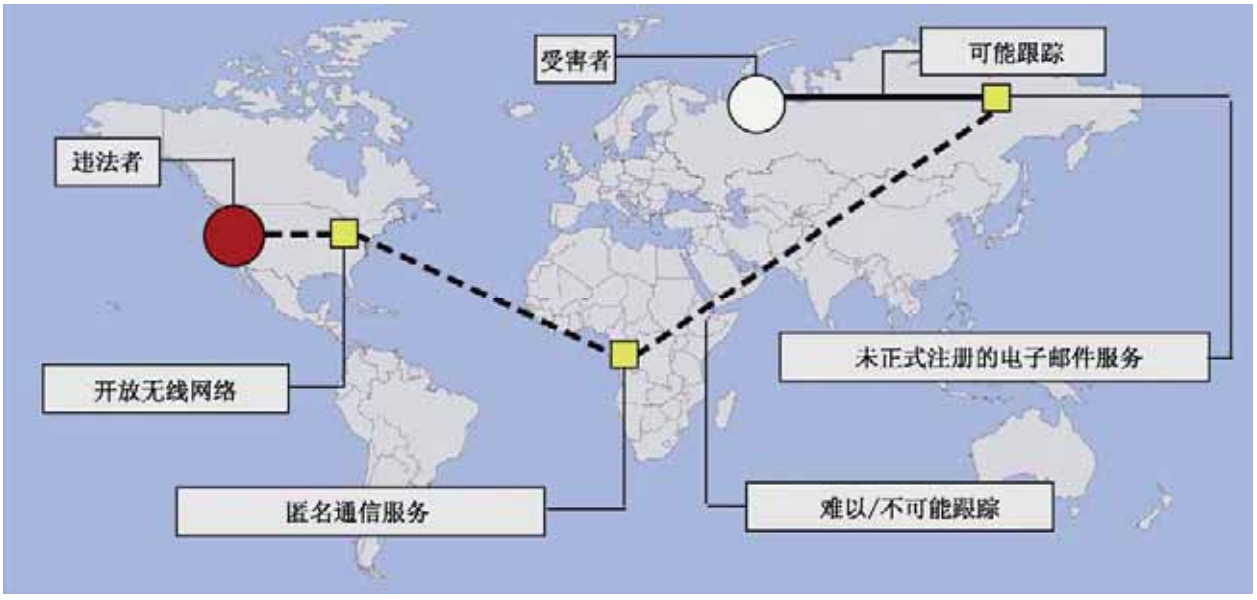
欲了解更多有关出版物的信息，请联系：

信息通信技术应用与网络安全处（CYB）
政策和战略部
电信发展局
国际电信联盟

Place des Nations
1211 Geneva 20
瑞士

电话：+41 22 730 5825/6052
传真：+41 22 730 5484
电邮：cybmail@itu.int
网址：www.itu.int/ITU-D/cyb/

国　　际　　电　　信　　联　　盟



了解网络犯罪：针对发展中国家的指南

国际电联电信发展部门
政策和战略部
信息通信技术应用与网络安全处

2009 年 4 月草案

欲了解更多信息，请联系

ITU-D 信息通信技术应用与网络安全处：cybmail@itu.int

国际电信联盟

缩 略 语

ABA	美国律师协会
APEC	亚太经济合作组织
APIG	所有方国际互联网集团
ASEAN	东南亚国家联盟
CFAA	计算机欺骗与滥用法案（美国）
CMA	计算机误用法案（英国），与计算机误用法案（新加坡）
CoE	欧洲理事会
DDoS	分布式拒绝服务
EC	欧洲委员会
EC 规则	隐私与电子通信规则 2003（英国）
ECPA	电子通信隐私法案（美国）
EU	欧洲联盟
G8	八国集团
GCA	全球网络安全议程
IAG	国际援助集团（加拿大）
ICT	信息通信技术
IRG	Gesetz über die Internationale Rechtshilfe in Strafsachen
ITU	国际电信联盟
OECD	经济合作与发展组织
OWig	Gesetz über Ordnungswidrigkeiten（德国）
PACC	ABA 隐私与计算机犯罪委员会
RIPA	调查权力规则法案（英国）
StGB	德国刑法（Strafgesetzbuch）
StPO	德国刑事程序法（Strafprozessordnung）
TKG	德国电信法案（Telekommunikationgesetz）
U.K.	英国
UN	联合国
UrhG	德国版权法案（Urheberrechtsgesecht）
U.S.	美国
WSIS	信息社会世界峰会

目　　的

国际电联出版物《**了解网络犯罪：针对发展中国家的指南**》（以下简称《指南》）旨在帮助各国了解网络安全方面的法律问题，并帮助协调法律框架。同样，《指南》旨在帮助发展中国家更好地了解有关日益增长之网络威胁在国家和国际层面的含义，评估现有国家、区域和国际层面机制的需求，帮助各国建立良好的法律基础。

《指南》全面论述了与网络犯罪法律方面问题最相关的各主题，重点在发展中国家的需求。由于网络犯罪的跨国特性，发展中国家和发达国家的法律文件是相同的。不过，选择使用的参考文献是针对发展中国家利益的。《指南》提供了一个很大的资源选择范围，以便更加深入地对不同的主题开展研究。无论何时，只要可能，都使用公开可用的资源，包括许多免费的在线法律期刊版本。

《指南》包含六个主要章节。引言之后（第 1 章），《指南》概述了网络犯罪现象（第 2 章），包括对网络犯罪如何实施的描述，并对最广泛的网络犯罪行为进行了解释，如黑客、身份盗用和拒绝服务攻击。《指南》还对面临的挑战做了描述，原因是它们与网络犯罪的调查与起诉有关（第 3 章和第 4 章）。在对国际和区域组织与网络犯罪行为进行斗争的若干活动进行概述之后（第 5 章），《指南》接着分析了有关实体刑法、程序法、国际互联网服务提供商国际合作与责任的不同法律方法（第 6 章），包括国际方法的例子，以及国家层面解决方案的良好范例。

《**了解网络犯罪：针对发展中国家的指南**》出版物论述国际电联全球网络安全议程（GCA）七个战略目标中的第一个目标，它呼吁精心安排有关制定网络犯罪法律的战略，使之全球适用、可实现与现有国家和区域法律体系的互操作；《指南》还论述了 ITU-D 研究组 Q22/1 用于组织国家网络安全工作的方法。建立适当的法律基础设施是国家网络安全战略的一个有机组成部分。所有国家都采用适当的法律，以防信息通信技术误用于犯罪或其他目的，包括旨在影响国家关键信息基础设施完整的活动，是实现全球网络安全的核心。由于网络威胁可来自全球的任何地方，因此面临的挑战本质上是面向国际范围的，为此需要国际合作、调查援助以及共同的实体法规和程序法规。因此，重要的是，各国之间协调好其法律框架，以便与网络犯罪作斗争，促进国际合作。

目　　录

1．引言 9

1.1 基础设施与服务 9
1.2 优势与风险 10
1.3 网络安全与网络犯罪 12
1.4 网络犯罪的国际影响 14
1.5 对发展中国家的影响 16

2． 网络犯罪现象 17

2.1 网络犯罪定义 17
2.2 网络犯罪类型 18
2.3 网络犯罪行为统计指标 19
2.4 破坏计算机数据与系统机密性、完整性和可用性的违法行为 20
2.4.1 非法访问（黑客行为、骇客行为） 21
2.4.2 数据刺探 23
2.4.3 非法截获 26
2.4.4 数据干扰 28
2.4.5 系统干扰 29
2.5 内容相关的违法行为 31
2.5.1 色情材料（不包括儿童色情） 32
2.5.2 儿童色情 34
2.5.3 种族主义、仇恨言论、鼓吹暴力 36
2.5.4 宗教违法行为 37
2.5.5 非法赌博与在线游戏 38
2.5.6 诽谤与虚假信息 40
2.5.7 垃圾信息与相关威胁 41
2.5.8 其他形式的非法内容 43
2.6 与版权和商标有关的违法行为 43
2.6.1 与版权有关的违法行为 44
2.6.2 与商标有关的违法行为 46
2.7 与计算机有关的违法行为 47
2.7.1 欺骗和与计算机有关的欺骗 48
2.7.2 与计算机有关的伪造 50
2.7.3 身份盗用 50
2.7.4 设备误用 53
2.8 组合违法行为 54
2.8.1 网络恐怖主义 55
2.8.2 网络战争 60

2.8.3 网络洗钱 61
2.8.4 网络钓鱼 63
2.9 网络犯罪的经济影响 64
2.9.1 所选调查结果概述 64
2.9.2 网络犯罪统计相关的困难 66

3. 与网络犯罪作斗争面临的挑战 67

3.1 机会 67
3.2 一般挑战 68
3.2.1 对信息通信技术的依赖 68
3.2.2 用户数量 69
3.2.3 设备与访问的可用性 70
3.2.4 信息的可用性 72
3.2.5 失去控制机制 73
3.2.6 国际影响 74
3.2.7 现场外的远程犯罪 75
3.2.8 自动化 76
3.2.9 资源 77
3.2.10 数据交换处理的速度 78
3.2.11 发展速度 79
3.2.12 匿名通信 80
3.2.13 加密技术 81
3.2.14 小结 83
3.3 法律挑战 83
3.3.1 在起草国际刑法方面的挑战 83
3.3.2 新的违法行为 84
3.3.3 越来越多的信息通信技术的应用与新的调查手段的需求 85
3.3.4 开发数字证据程序 85

4. 反网络犯罪战略 87

4.1 将网络犯罪立法作为网络安全战略的一部分 87
4.2 现有战略的实施 88
4.3 区域差异 88
4.4 网络安全支柱内网络犯罪问题的关联性 89
4.4.1 法律措施 89
4.4.2 技术与程序措施 89
4.4.3 组织结构 90
4.4.4 能力建设与用户教育 91
4.4.5 国际合作 92

5. 国际法律方法概述 93
5.1 国际方法 93
5.1.1 八国集团 93
5.1.2 联合国 95
5.1.3 国际电信联盟 97
5.1.4 欧洲理事会 99
5.2 区域方法 101
5.2.1 欧盟 101
5.2.2 经济合作与发展组织 106
5.2.3 亚太经济合作组织 107
5.2.4 英联邦 108
5.2.5 阿拉伯联盟与海湾合作理事会 109
5.2.6 美洲国家组织 109
5.3 科学方法 111
5.4 不同国际与法律方法之间的关系 111
5.5 国际与国家法律方法之间的关系 113
5.5.1 国家方法得以普及的原因 113
5.5.2 国际解决方案对国家解决方案 114
5.5.3 国家方法的困难 114
6. 法律响应 116
6.1 实体刑法 116
6.1.1 非法访问（黑客行为） 116
6.1.2 数据刺探 121
6.1.3 非法截获 123
6.1.4 数据干扰 127
6.1.5 系统干扰 131
6.1.6 色情材料 135
6.1.7 儿童色情 137
6.1.8 仇恨言论、种族主义 142
6.1.9 宗教违法行为 145
6.1.10 非法赌博 147
6.1.11 侮辱与诽谤 150
6.1.12 垃圾邮件 152
6.1.13 设备误用 154
6.1.14 与计算机有关的伪造 160
6.1.15 身份盗用 163
6.1.16 与计算机有关的欺骗 166
6.1.17 版权犯罪 169

6.2 程序法 172
6.2.1 引言 172
6.2.2 计算机与国际互联网调查（计算机取证） 173
6.2.3 保护措施 175
6.2.4 加速保存与透露保存的计算机数据（快速冻结） 179
6.2.5 数据保留 184
6.2.6 搜查与查封 188
6.2.7 提供数据命令 193
6.2.8 实时收集数据 196
6.2.9 收集通信流量数据 197
6.2.10 截获内容数据 199
6.2.11 有关加密技术的规定 201
6.2.12 远程取证软件 206
6.2.13 授权要求 208
6.3 国际合作 209
6.3.1 引言 209
6.3.2 国际合作的一般原则 209
6.3.3 引渡 210
6.3.4 相互援助的一般原则 211
6.3.5 在无适用的国际协议情况下关于相互援助请求的程序 212
6.3.6 关于临时措施的相互援助 213
6.3.7 跨界访问所储存的计算机数据 214
6.3.8 24/7 联系网络 215
6.3.9 《斯坦福公约》草案中的国际合作 217
6.4 国际互联网提供商的责任 217
6.4.1 引言 217
6.4.2 美国方法 218
6.4.3 欧盟有关电子商务的指令 220
6.4.4 访问提供商的责任（欧盟指令） 221
6.4.5 缓冲的责任（欧盟指令） 221
6.4.6 托管服务提供商的责任（欧盟指令） 222
6.4.7 排除监控职责（欧盟指令） 223
6.4.8 超链接的责任（奥地利 ECC） 224
6.4.9 搜索引擎的责任 225
7. 法律参考文献 226

1. 引言

1.1 基础设施与服务

国际互联网是技术基础设施发展中增长最快的领域。[1] 今天，信息通信技术（ICT）已经无处不在，而且数字化的趋势仍在进一步增长。对国际互联网和计算机连接性的需求，已经引领计算机技术集成到一些产品中，如汽车和建筑物，[2] 本来这些产品没有计算机技术也能发挥作用。电力供应、交通基础设施、军事作战与保障 — 事实上，所有现代服务都依赖信息通信技术的使用。[3]

尽管新技术的发展主要用于满足西方国家消费者的需求，但发展中国家也同样从中受益。[4] 诸如 WiMAX [5] 之类的远程无线通信技术以及计算机系统（现在的价格已经不到 200 美元）[6] 的可用性，使越来越多的发展中国家的人们能够更加方便地接入国际互联网、享用相关的产品和服务。[7]

信息通信技术对社会的影响远远超过建立基本的信息基础设施。信息通信技术的可用性是在创建和使用基于网络之服务的发展过程中的基础，[8] 电子邮件已经取代了传统的信件；[9] 如今，对企业而言，在线的互联网展示已经比打印的广告材料更为重要；[10] 基于国际互联网的通信以及电话服务正以比陆地线路通信速度更快的速度在增长。[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", 2006,

总的来说，信息通信技术以及新的基于网络的服务的可用性，为社会带来了众多优势，特别是对发展中国家。

诸如电子政务、电子商务、电子教育、电子健康和电子环境等信息通信技术应用，已被人们视为发展的助推器，原因是它们为向偏远和农村地区提供各种各样的基础服务提供了一条有效的渠道。信息通信技术的应用有助于推动千年发展目标的实现、减少发展中国家的贫困、改善健康和改善条件。运用正确的方法、背景和执行过程，在信息通信技术应用与工具中的投资可以带来生产力和质量的提升。反过来，信息通信技术的应用可以释放技术与人类的能力，使基本服务更具可达性。在这方面，出于犯罪目的、抱着诈骗的意图，借助国际互联网来实施在线的身份盗用和获取他人证书和/或个人信息的行为，现已成为电子政务和电子商务服务进一步发展的主要威胁之一。[12]

国际互联网服务的成本通常也大大低于网络之外可比服务的成本。[13] 与传统的邮政服务相比，电子邮件服务通常是免费的，或者只收取非常少的一点费用。[14] 在线的维基百科服务[15] 也可以免费使用，还包括数百种的在线托管服务。[16] 低成本相当重要，原因是这使得更多的用户可以使用这些服务，包括那些只有有限收入的人们。鉴于发展中国家许多人有限的财力，国际互联网使得他们能够使用一些在网络之外无法以如此低廉价格得到的服务。

1.2 优势与风险

在日常生活的诸多方面中引入信息通信技术已经带来信息社会这一现代概念的提出。[17] 信息社会的发展提供了巨大机遇。[18] 无障碍地访问信息有助于民主，原因是信息的流动不受国家政权的控

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.

制（如在东欧国家发生过的情况）。[19] 技术发展改善了日常生活 — 例如网上银行和网上购物、移动数据业务和网络协议语音服务（VoIP）的使用，就是信息通信技术如何融入我们日常生活的一些例子。[20]

不过，信息社会的发展也伴随着新的和严重的威胁。[21] 如今，人类生活中一些必不可少的服务，如供水和电力供应等，都依赖于信息通信技术。[22] 汽车、交通管制、电梯、空调和电话等，也都依赖于信息通信技术流畅地发挥其功能。[23] 对信息基础设施和国际互联网服务的攻击现已具有以新的和危险的方式危害社会的可能性。[24]

对信息基础设施和国际互联网服务的攻击已有发生。[25] 网络诈骗、传播儿童色情以及黑客攻击等，只是与计算机有关的犯罪的一些例子，如今，这类犯罪每天都会大量发生。[26] 网络犯罪导致巨额的经济损失。[27] 仅 2003 年一年，恶意软件就造成了高达 170 亿美元的损失。[28] 据估计，2007 年，网络犯罪带来的收入超过了 1000 亿美元，第一次超过了毒品非法贸易的收入。[29] 接近 60%的美国企业认为，网络犯罪比其他物理犯罪对其造成的危害更大。[30] 这些预计清楚地表明了保护好信息基础设施的重要性。[31]

---

[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.

[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 网络安全与网络犯罪

网络安全[32]在当前的信息技术以及国际互联网服务[33]的发展中发挥着重要作用。增强网络安全和保护关键的信息基础设施，对各国安全和经济福利至关重要。使国际互联网更加安全（并且保护国际互联网用户），已经成为新业务发展和各国政策的有机组成部分。[34] 阻止网络犯罪是国家网络安全和关键信息基础设施保护战略的有机组成部分。特别地，这包括采取适当的立法措施，阻止出于犯罪或其他目的滥用信息通信技术，以及防止那些旨在影响国家关键基础设施完整性的行为。在国家层面上，这是一种共同的责任，要求政府主管部门、私营部门和公民各方在阻止、预备、响应和恢复网络犯罪方面采取协同行动。在区域和国际层面上，这需要各相关方的合作与协调。因此，在网络安全的国家框架与战略的形成和实施上，需要采取一种综合的方法。[35] 网络安全战略 — 例如，技术保护系统的研发，或者教育用户如何预防成为网络犯罪的受害者 — 将有助于降低网络犯罪的风险。[36] 制定和支持网络安全战略是在与网络犯罪作斗争的过程中一个至关重要的因素。[37]

由网络安全问题引发的法律上、技术上和制度上的挑战，是全球性的和深远的，并且只有在国际合作的框架内，考虑到不同利益相关方和现有举措的作用，通过一种一致的战略才能加以解决。[38]

---

[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 of the ITU Global Cybersecurity Agenda, 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.

在这方面，信息社会世界峰会（WSIS）[39] 已认识到因网络安全的缺陷和网络犯罪的泛滥而导致的真实而巨大的风险。《**信息社会世界峰会信息社会突尼斯议程**》[40] 第 108～110 段，包括附录，为利益相关各方在国际层面上执行《**信息社会世界峰会日内瓦行动计划**》[41] 制定了一个计划，计划根据 11 条行动线以及为便于不同行动主线的实施而分配的责任，描述了利益相关各方的实施过程。在信息社会世界峰会上，世界各国领导人和政府指派国际电信联盟推动信息社会世界峰会行主线 C5 的执行，并致力于在信息通信技术使用过程中建立信息、确保安全。[42]

在这方面，国际电信联盟秘书长与来自政府、业界、区域以及国际组织、学术与研究机构的合作伙伴一道，于 2007 年 5 月 17 日签署了《全球网络安全议程》（GCA）。[43] 《全球网络安全议程》是一个有关对话与国际合作的全球框架，旨在协调国际社会对日益严峻的网络安全挑战做出响应，以及增强信息社会的信心和安全。它基于现有的工作、举措和合作关系，目标是提出全球战略，以应对当前与使用信息通信技术建立信心和安全有关的挑战。在国际电联内，通过在国际合作框架内促进国际电联三个部门对网络安全活动的执行，《全球网络安全议程》补充了现有的国际电联工作计划。

GCA 有七大战略目标，建立在五个工作领域之上：1）法律措施；2）技术与程序措施；3）组织结构；4）能力建设；以及 5）国际合作。[44]

与网络犯罪的斗争需要一种综合的方法。鉴于任何一种技术措施都无法单独防止任何犯罪，因此，允许执行机构对网络犯罪进行有效调查和起诉至关重要。[45] 在 GCA 的工作领域中，“法律措施”着眼于如何应对网络犯罪活动带来的挑战，这些犯罪是以国际兼容的方式、在信息通信技术网络上进行的。“技术与程序措施”着眼于关键举措，以便采取更好的方法，增强和改善网络空间的安全与风险管理，包括认证计划、协议和标准。“组织结构”着眼于预防、探测、响应网络攻击并做好危机管理，包括保护关键的信息基础设施系统。“能力建设”着眼于精心制定有关能力建设机制的战略，以便在国家政策议程中提高意识、传播技能、促进网络安全。最后，“国际合作”着眼于在应对网络威胁中的国际合作、对话和协调。

制定适当的法律以及在这种方法内制定与网络犯罪有关的法律框架，是网络安全战略的一个重要组成部分。这首先要求所有必需的实体刑法条款来对一些行为定罪，如计算机诈骗、非法访问、数据干扰、版权侵权和儿童色情。[46] 事实是，适用于类似之非网络犯罪行为的刑法条款，并不意味

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

着也可适用于国际互联网上的犯罪行为。[47] 因此，对当前的国家法律进行全面彻底的分析，对辨别任何可能存在的差别至关重要。[48] 除了实体刑法条款，[49] 执法机构还需要一些必要的工具和设备来调查网络犯罪。[50] 而此类调查本身就带来了一系列的挑战。[51] 罪犯几乎可以从世界任何地方来实施犯罪行为，并采取措施掩盖其身份。[52] 与那些用来调查普通犯罪行为的工具和设备相比，调查网络犯罪行为所需的工具和设备可能大不相同。[53]

1.4 网络犯罪的国际影响

网络犯罪常常波及国际范围。[54] 带有非法内容的电子邮件，在从发送者传送到接收者的过程中，常常历经许多国家，或者非法内容可以保存在别的国家。[55] 在网络犯罪调查过程中，相关国家之间的密切合作极为重要。[56] 各国之间现有的相互法律援助协议基于正式的复杂的且常常是耗时的程序。[57] 因此，至关重要的是，建立一些有助于对网络犯罪案件迅速做出响应且请求国际合作的程序。[58]

[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; 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.

许多国家将其相互法律援助体系建立在“双重犯罪”的原则上。[59] 全球层面上对网络犯罪的调查通常局限于在所有参与国家中已定罪的那些犯罪。尽管许多攻击行为可能在世界任何地方都会遭到起诉，但区域之间的差别扮演着重要的角色。[60] 非法内容就是一个例子。不同国家对非法内容的定罪就有差别。[61] 在某个国家中可以合法传播的内容，在另一个国家很可能就是非法的。[62]

当前正在使用的计算机技术基本上是世界通用的。[63] 除了语言问题和电源适配器的不同，亚洲和欧洲销售的计算机系统和手机几乎没有什么差别。国际互联网世界也是类似的情形。由于标准化的实施，非洲各国使用的协议与美国使用的协议是相同的。[64] 标准化使世界各地的用户能够通过国际互联网接入相同的服务。[65]

问题是全球技术标准化的一致对国家刑法的发展将产生怎样的影响。就非法内容而言，国际互联网用户可以从世界各地访问信息，这样，他们能够访问在国外属于合法而在本国属于非法的信息。

理论上，来自技术标准化的发展远超过了技术与服务的全球化，并且可能导致各国法律的调和。不过，正如在欧洲委员会《网络犯罪公约》第一协议的谈判过程中所示的那样，[66] 国家法律原则的变化远比技术发展的步伐慢得多。[67]

---

[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.

[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/T061500000A0015P
DFE.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.

尽管国际互联网并不认可国界控制，但的确存在一些手段可限制对特定信息的访问。[68] 接入提供商通常可以阻止某些网站，而保存了某一网站的服务提供商，可以根据与某一特定国家相关联的 IP 地址，阻止那些用户访问其信息（“IP 筛选”）。[69] 两种措施都可以被绕开，但是不管怎样，它们是可以用来在全球网络中保持地区差别的手段。[70] 开放网络倡议[71] 报告说，全世界约有 24 个国家实施这种审查制度。[72]

1.5 对发展中国家的影响

寻求应对网络犯罪威胁的战略与解决方案是一个重大挑战，对于发展中国家尤其如此。综合的反网络犯罪战略通常包括技术保护措施以及法律手段。[73] 这些手段的制定与实施需要时间。技术保护措施尤其需要高额的成本。[74] 发展中国家需要从一开始就将保护措施溶入到国际互联网的普及中，原因是，尽管这可能在最初提高国际互联网服务的成本，但从长期看，由于避免了因网络犯罪而造成的巨大费用和破坏，其收益将大大超过任何技术保护措施和网络安全防卫措施的初始成本。[75]

事实上，由于发展中国家不太严格的安全和防护措施，与脆弱的保护措施有关的风险可能更严重地影响到它们。[76] 有能力保护客户和公司，不仅仅是一项针对日常业务的基本要求，也是针对在线或基于国际互联网业务的基本要求。如果缺乏国际互联网安全性，发展中国家可能在推动电子商务和进军在线服务行业等方面遭遇巨大困难。

发展有助于网络安全的技术措施以及制定适当的有关网络犯罪的法律，对发达国家和发展中国家都至关重要。相比之后才在计算机网络中采取安全和保护措施所耗费的成本，一开始就采取网络安全防护措施其成本将便宜得多。发展中国家需要将其反网络犯罪战略在一开始就与国际标准保持一致起来。[77]

---

[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.

[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. 网络犯罪现象

2.1 网络犯罪定义

关于网络犯罪的大多数报告、指南或出版物都以定义“网络犯罪”这一术语开始。[78] 一种常见的定义是将网络犯罪描述成以计算机或网络为工具、目标或地点的任何犯罪活动。[79] 国际上常见的一个例子是《加强预防网络犯罪和恐怖主义（CISAC）[80] 国际公约》草案第 1.1 条中的定义，它将网络犯罪定义为涉及网络系统的犯罪行为。[81] 有些定义试图将网络犯罪的目标或意图考虑进来，对网络犯罪做更准确的定义，[82] 将其定义为“非法的或被某些团体视为不正当的、可以通过全球电子网络实施的、以计算机为媒介的行为。”[83]

这些更加精确的描述没有包括那些利用物理硬件来实施的普通犯罪，而这存在一定风险，因此这些犯罪行为有可能被一些国际协议认定为网络犯罪，如《网络犯罪公约》。[84] 例如，如《欧洲理

[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] *Article* 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*.

事会关于网络犯罪的公约》定义，若某人生产包含恶意软件的 USB[85] 设备，当该设备被连接时对计算机数据造成破坏，那么认为他在实施一种犯罪行为。[86] 不过，根据以上狭义定义，没有通过全球电子网络进行的、使用物理设备来删除数据以复制恶意代码的行为，将不被定性为网络犯罪。而根据更宽泛的描述和定义，不仅这种行为被定义为网络犯罪，而且包括如非法的数据干扰等行为也被定义为网络犯罪。

这表明，在定义“网络犯罪”这一术语上，存在极大的困难。[87] “网络犯罪”这一术语用于描述一系列的攻击行为，包括传统的计算机犯罪以及网络犯罪。由于这些犯罪行为在许多方面存在差异，因此没有哪一种单独的准则能够将《斯坦福公约》草案以及《网络犯罪公约》中提到的所有行为都包括在内，且不包括那些只是使用硬件实施的传统的犯罪行为。事实上，只要这一术语不是用作法律术语，那么使用哪一种定义并不重要。[88]

2.2 网络犯罪类型

“网络犯罪”这一术语包括一系列犯罪行为。[89] 公认的犯罪行为涵盖众多的犯罪行为，使得难以为网络犯罪制定一套分类或归类体系。[90] 可以在《欧洲理事会关于网络犯罪的公约》中找到一套有趣的分类体系。[91] 《网络犯罪公约》对以下四种类型的犯罪行为做了区分：[92]

[85] Universal Serial Bus (USB)

[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.

- 破坏计算机数据与系统机密性、完整性和可用性的攻击行为；[93]
- 与计算机有关的攻击行为；[94]
- 与内容有关的攻击行为；[95] 以及
- 与版权有关的攻击行为；[96]

这种分类整体上并不一致，原因是它没有基于一个单独的标准来区分各个类别。三个类别着重强调法律保护的目标："破坏计算机数据与系统机密性、完整性和可用性的攻击行为"；[97] 与内容有关的攻击行为；[98] 以及与版权有关的攻击行为。[99] 第四个类别"与计算机有关的攻击行为"[100] 不是着重于法律保护的目标，而是着眼于犯罪方法。这种不一致性导致各类别之间存在一定的重叠。

此外，用于描述犯罪行为的一些术语（例如"网络恐怖主义"[101] 或者"网络钓鱼"[102]），涵盖了可同时归入几个类别的犯罪行为。尽管如此，《网络犯罪公约》提供的分类仍是讨论网络犯罪现象的有用依据。

2.3 网络犯罪行为统计指标

网络犯罪对社会产生的影响难以进行量化。[103] 因网络犯罪造成的经济损失以及攻击行为的数量十分难以估计。某些渠道估计，美国的企业和机构[104] 因网络犯罪而造成的损失高达 670 亿美元之多；不过，难以肯定对抽样调查结果所做的推断是否合理。[105] 对这种方法论的批判不仅适用于损失，而且适用于工人的攻击数量。[106]

[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.
[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.

由于攻击对象不会总是报告这些攻击行为，因此难以度量网络犯罪的数量。[107] 尽管如此，调查有助于理解网络犯罪的影响。通过比较几年内的数量来得出比来自任何一年内数量更准确、更相关的、有关网络犯罪的数量结果是未来的一种发展趋势。

一个例子是美国计算机安全协会（CSI）[108] 于 2007 年进行的计算机犯罪与安全调查，该调查分析了与计算机有关的攻击行为的数量。[109] 调查基于来自美国公司、政府机构和金融机构 494 个计算机安全从业者的回复。[110] 调查文件记录了答复者报告的、在 2000 年至 2007 年之间发生的攻击行为数量。调查结果显示，自 2001 年以来，经历并承认受到过病毒攻击或非授权信息访问（或系统渗透）的答复者的比例下降了。调查结果没有解释为什么出现了这种下降趋势。不过，来自其他机构的调查结果也支持这种提及之分类中认可的攻击数量出现下降的现象（这与媒体有时报告的情况正好相反）。[111] 通过分析犯罪统计数据，也可发现类似的趋势 — 例如，德国的犯罪统计数据[112] 表明，在 2004 年达到峰值之后，与计算机有关的攻击行为的数量已经减少到接近 2002 年的水平。

关于网络犯罪的统计数据无法提供有关攻击行为程度或范围的可靠信息。[113] 由于无法确定攻击对象报告的攻击程度，[114] 以及由于以下事实，即无法找到关于网络犯罪数量减少的合理解释，因此，这些统计数据任由人们去解读。目前，没有足够的证据来预测未来的趋势和发展。

2.4 破坏计算机数据与系统机密性、完整性和可用性的违法行为

归入这一类别的所有攻击行为，都是针对机密性、完整性和可用性这三条法律原则中的（至少）一条。与数个世纪以来刑法中所涵盖的犯罪（如盗窃和谋杀）不同，犯罪行为的计算机化出现的时间相对较晚，原因是计算机系统和计算机数据的发展只是大约 60 年前的事情。[115] 对这些犯罪行为进行有效的起诉要求现有的刑法条款不仅保护有形的实体和物理的文件不被操纵，而且还要延伸至纳入这些新的法律原则。[116] 本小节对这一类别中包含的、最常见的攻击行为做一概述。

---

[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.

[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."

2.4.1 非法访问（黑客行为、骇客行为）[117]

描述为“黑客行为”的攻击行为指的是非法访问计算机系统，[118] 这是一种最早出现的、与计算机有关的犯罪行为。[119] 随着计算机网络的发展（特别是国际互联网），这种犯罪行为已经变得日益普遍。[120] 黑客攻击的一些著名对象包括美国国家航空航天局（NASA）、美国空军、五角大楼、雅虎、谷歌、易趣（eBay）以及德国政府等。[121] 黑客攻击的例子包括：

- 破解受到密码保护的网站的密码[122]；以及
- 绕过计算机的密码保护。

准备行为的例子包括：

- 使用有缺陷的硬件或执行有缺陷的软件来非法获取密码以进入计算机系统；[123]
- 创建“诱骗”网站以使用户泄露其密码；[124] 以及
- 安装基于键盘记录方法的硬件和软件（如“键盘记录器”）记录每一次键盘敲击 — 并因此盗取在计算机和/或设备上使用的任何密码。[125]

图1

图1 图形显示网站被黑了。攻击者修改了首页，告诉用户攻击成功。

[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/Lotriont*e, 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.
[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.

攻击者的动机各不相同。一些攻击者将其行为局限于绕过安全措施的活动，只是为了证明自己的能力（如图 1 所示）。[126] 其他攻击者的行为带有政治意图（称为“黑客行动主义”[127]） — 一个例子是最近攻击联合国主要网站的事件。[128] 在大多数情况下，攻击者的动机不会仅限于不正当地访问计算机系统。攻击者利用这种访问来实施进一步的犯罪，如数据刺探、数据操纵或拒绝服务（DoS）攻击。[129] 在许多情况下，对计算机系统的非法访问只是网络犯罪至关重要的第一步。[130]

许多分析人士认识到，试图非法访问计算机系统事件的数量正在增加，仅 2007 年 8 月一个月，全世界就报告了超过 2500 万件此类案件。[131] 导致黑客攻击案件数量增加的主要因素有三个：

计算机系统的保护措施不力和不完整：

全世界有数亿台计算机与国际互联网连接，许多计算机系统不具备适当的保护措施以防止非法访问。[132] 美国马里兰大学进行的一项分析表明，连接到国际互联网的、未采取保护措施的计算机系统，有可能在不到一分钟的时间内就遭到攻击。[133] 安装保护措施可以降低被攻击的风险，但对那些具有良好保护措施的计算机系统进行的成功攻击证明，技术保护措施绝不能彻底阻止攻击。[134]

自动攻击软件工具的发展：

最近，正用软件工具来自动发起攻击。[135] 在软件和预先设定的攻击的帮助下，单独一个攻击者可以使用一台计算机、在一天内向数千台计算机系统发动攻击。[136] 如果攻击者访问更多的计算机 — 例如通过僵尸网络[137] — 他/她可以进一步扩大攻击范围。由于这些软件工具中的大多数使用预先设定的攻击方法，因此并非所有的攻击都证明是成功的。定期更新操作系统和软件应用程序的用户，可以降低其成为这些大规模攻击的受害者的风险，原因是开发保护软件的公司对攻击工具进行了分析，并对标准化的黑客攻击行为有所防范。

---

[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.

[134] For an overview of examples of successful hacking attacks, see http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriontе*, 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.

明确的攻击常常基于个别设计的攻击。这些攻击之所以成功，并不是什么采用了高精尖方法的结果，而在于被攻击计算机系统的数量。能够实现这些标准化攻击的工具在国际互联网上随处可见[138]有些是免费的，但有效的工具往往要花费几千美元。[139]一个例子是一种可以使攻击者定义一个IP地址范围（例如从111.2.0.0到111.9.253.253）的黑客攻击工具。这些软件能够对使用其中一个定义之IP地址的所有计算机的未保护端口进行扫描。[140]

在黑客策略中个人计算机越来越成为攻击目标：

访问一个计算机系统通常并不是攻击的主要动机。[141]由于商业计算机通常比个人计算机保护得更好，因此，更难使用预先配置的软件工具对商业计算机实施攻击。[142]过去几年间，攻击者逐渐将其攻击对象指向个人计算机，原因是许多个人计算机都没有采取足够的保护措施。此外，个人计算机通常包含敏感信息（例如信用卡和银行账号细节）。攻击者也以个人计算机为目标，是因为在一次成功的攻击之后，攻击者可以将这台计算机纳入其僵尸网络中，并将其用于实施进一步的犯罪活动。[143]

非法访问计算机系统可被视为与非法闯入某一建筑物相类似，在许多国家，这被认为是刑事犯罪行为。[144]对非法访问计算机行为的定罪有许多不同方法，对这些方法的分析表明，在某些情况下制定的法律条款将非法访问与随后的攻击行为相混淆了，或者试图将非法访问的定罪仅仅限制为严重违法而已。有些规定只对最初的访问定罪，而其他方法仅将刑事犯罪限定为以下情形：

- 被访问的系统受到安全措施的保护；[145]和/或
- 攻击者具有恶意；[146]和/或
- 获取、修改或破坏了数据。

其他的法律体系没有对单纯的访问予以定罪，而着重于随后的攻击行为。[147]

2.4.2 数据刺探

计算机系统中常常保存有敏感信息。如果计算机系统与国际互联网相连，那么攻击者可以借助国际互联网，从世界几乎任何地方试图访问到这些信息。[148]国际互联网越来越多地用于获取贸易秘

[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.
[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.

密。[149] 敏感信息的价值以及远程访问之的能力使得数据刺探变得极有兴趣。20 世纪 80 年代，许多德国的黑客成功地进入到了美国的政府和军事计算机系统，获取了秘密情报并将它们卖给了苏联的情报机构。[150]

攻击者使用各种各样的技术来访问受害者的计算机，[151] 包括：

- 利用软件来扫描未保护的端口；[152]
- 利用软件来绕过保护措施；[153] 以及
- 运用“社会工程”。[154]

尤其是最后一种方法“社会工程”，指的是一种非技术型的入侵方法，它在很大程度上依赖于人的互动，通常引诱人们违反正常的安全程序，因此格外有趣，原因是它不基于技术性手段。[155] 对于采取了良好保护措施的计算机系统，“社会工程”方法也绝不是不太有效的方法。它进一步描述了对人的操纵，意图是获得对计算机系统的访问。[156] 社会工程通常极为成功，原因是计算机安全中最薄弱的环节常常就是操作计算机系统的用户。

例如，“网络钓鱼”最近成为网络空间中一种重要的犯罪行为，[157] 它指的是试图以欺诈手段获取敏感的信息（如密码），方法是在一次看似正式的电子通信中，伪装成一个可信任的人或者一家可信任的企业（如金融机构）来实施欺诈。

尽管用户在人性方面的弱点为网上实施欺骗打开了方便之门，但它也提供了解决方案。经过良好教育的计算机用户不会轻易成为攻击者的受害对象。用户教育是任何一种反网络犯罪战略的重要组成部分。[158] 经济合作与发展组织（OECD）强调用户使用加密技术的重要性，原因是加密技术有

---

[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.

[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.

助于加强数据保护。[159] 如果存储信息的个人或组织使用适当的保护措施，那么密码保护措施将比任何物理的保护措施更为有效。[160] 攻击者成功获取敏感信息常常是由于被攻击对象缺少保护措施。

尽管攻击者通常以商业秘密为目标，但保存在个人计算机上的数据也正日益成为攻击对象。[161] 个人用户通常会在其计算机上保存银行账号和信用卡信息。[162] 攻击者可以将这些信息用于其自身目的（例如，获取银行账号详细信息以转移资金）或者将其卖给第三方。[163] 例如，信用卡记录的出售价格可高达 60 美元。[164] 黑客对个人计算机的关注非常有趣，原因是来自商业秘密的利润通常高于靠获取或出卖个人信用卡信息而获得的利润。不过，由于个人计算机通常缺乏严密的保护，因此对个人计算机进行数据刺探可能变得更加有利可图。

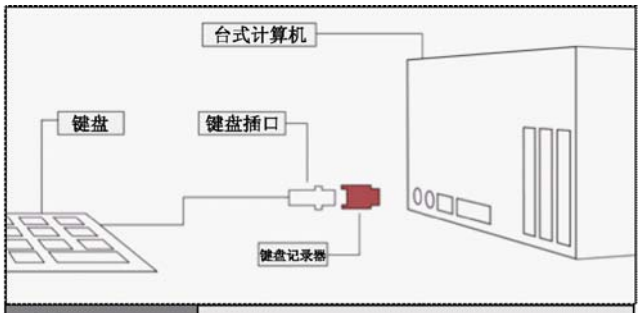


图2

图形显示如何安装硬件形式的键盘记录器。大多数此类工具—看起来像适配器—置于键盘插口与计算机之间。一些最新的形式是含在键盘内，因此若不打开硬件则无法发现它们。防病毒软件产品无法识别基于硬件形式的键盘记录器。

获取信息的手段有两种：

- 访问计算机系统或数据存储设备并获取信息；或者
- 运用操纵方法来使用户泄露信息或访问代码，使攻击者能够访问信息（“网络钓鱼”）。

攻击者常常使用安装在受害者计算机上的计算机工具或者一种称为“刺探程序”的恶意软件来向自己传输数据。[165] 最近几年，出现了各种类型的刺探程序，如键盘记录器。[166] 键盘记录器是一种记录受感染计算机的键盘上每一次键盘敲击的软件工具。[167] 有些键盘记录器只要受害者的计算机连接到国际互联网，便可向攻击者发送所有记录的信息。另一些键盘记录器对记录的数据进行初步整理和分析（例如，只选取可能是信用卡信息的数据[168]），只传输发现的重要数据。

---

[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_cooperation/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.

[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.

类似的设备也可以像硬件设备一样插入键盘与计算机系统之间，以记录键盘上的敲击（参见图 2）。基于硬件的键盘记录器更难安装和检测，原因是它们需要物理接入计算机系统。[169] 不过，传统的反刺探程序和反病毒软件基本上无法识别它们。[170]

除了访问计算机系统，攻击者还可以通过操纵用户来获取数据。最近，攻击者研发了一些有效的欺骗诡计来获取秘密信息（如银行账号信息和信用卡数据），方法是利用社会工程技术来操纵用户。[171] 最近，“网络钓鱼”已成为与网络空间有关的一种最重要的犯罪行为。[172] “网络钓鱼”这一术语用于描述这样一种犯罪类型，即它试图通过欺诈手段来获取敏感信息，例如，在一次看似正规的电子通信中通过伪装成一个可信任的人或一家可信任的企业（如金融机构）来获取密码等。[173]

数据刺探是网络犯罪的又一个例子，攻击者狡猾地瞄准计算机安全中的一个最薄弱环节 — 用户。考虑这一点，可以清楚地展示这些欺骗诡计的风险。但它也为解决方案找到了出路。受过良好教育的计算机用户不会轻易成为攻击者的受害对象。这突出了用户教育的重要性，它是任何一种反网络犯罪战略的重要组成部分。[174]

敏感信息正越来越多地保存在计算机系统中。因此，评估用户所用的技术保护措施是否恰当，或者立法者是否需要通过对数据刺探行为定罪以建立额外的保护措施，就显得至关重要。[175]

2.4.3 非法截获

攻击者可以截获用户之间的通信[176]（如电子邮件）或者截获数据传输（当用户在网络服务器上下载数据或访问基于互联网的外部存储媒介时[177]），以记录所交换的信息。攻击者能够以任何通信基础设施（如固定线路或无线通信）以及任何国际互联网服务（如电子邮件、网络聊天或 VoIP 通信[178]）为攻击对象。

---

[169] One approach to gain access to a computer system to install a key-logger is for example 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 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.

在国际互联网基础设施提供商或国际互联网服务提供商中进行的大多数数据传输过程都得到了良好的保护，难以截获。[179] 不过，攻击者寻找系统中的弱点。无线技术正越来越受欢迎，但在过去，它被证明是脆弱的。[180] 如今，宾馆、酒店和酒吧都为客户提供了通过无线接入点接入国际互联网的服务。不过，在计算机与接入点之间交换数据的信号可以在方圆 100 米的范围内被截获。[181] 想要截获数据交换过程的攻击者，可以在这一半径范围内的任何地方做到这一点（如图 3 所示）。即使无线通信采用了加密技术，攻击者也能够对记录的数据进行解密。[182]

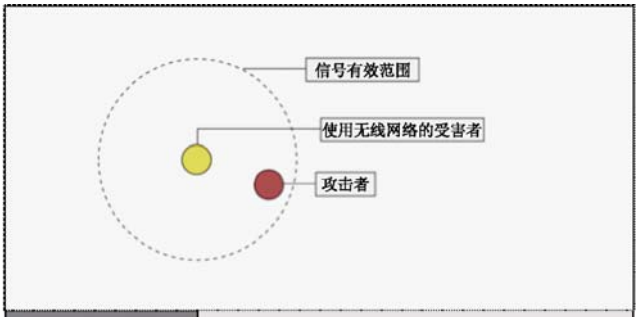


图3

图形显示的是一种针对使用无线网络连接的计算机用户进行攻击的情形。企图截获发送和接收数据的攻击者可以从信号有效范围内的任何位置发起攻击。依据无线路由器及其位置，信号甚至可以在100米半径范围内接收到。

为了获取敏感信息，有些攻击者将接入点设在无线访问需求很大的地方附近 [183]（如邻近的酒吧和酒店）。常常以以下方式来命名站点的位置，即寻求国际互联网接入点的用户更有可能选择欺诈的接入点。如果用户依靠访问提供者来确保其通信的安全，而不是执行其自身的安全措施，那么攻击者可以轻易地截获通信内容。

使用固定线路不能防止攻击者截获通信流量数据。[184] 通过电缆进行的数据传输会辐射电磁能量。[185] 如果攻击者使用恰当的设备，那么可以检测和记录这些辐射，[186] 并且能够记录下用户计算机与所连接系统之间的数据传输，而且也在计算机系统内。[187]

大多数国家已经开始保护对电信服务的使用，方法是对非法截获电话通话行为予以定罪。不过，鉴于基于 IP 的服务日益普及，立法者可能需要评估应当为基于 IP 的服务提供怎样的类似保护。[188]

[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 数据干扰

计算机数据对于个人用户、企业和主管部门而言都是至关重要的，原因是他们都要依赖数据的完整性和可用性。[189] 无法访问数据可导致巨大的（财政）损失。攻击者可破坏数据的完整性并借助以下方法对数据进行干扰：[190]

- 删除数据；和/或
- 隐瞒数据；和/或
- 更改数据；和/或
- 限制对数据的访问。

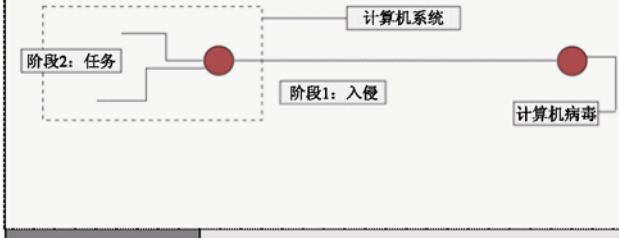


图4

图形显示了计算机病毒的作用过程。在感染计算机系统后（阶段1），病毒完成计划的任务（阶段2）。例如，这可以是删除或加密某些文件。

删除数据的一个常见例子是计算机病毒。[191] 自从计算机技术问世以来，计算机病毒就对那些没有安装适当保护措施的用户构成了威胁。[192] 自那时起，计算机病毒的数量发生了巨大的增长。[193] 最近，在两个主要方面发生了重大变化：

- 病毒的传播方式；以及
- 有效载荷。[194]

过去，计算机病毒通过存储设备来传播，如软盘，而如今，大多数病毒则通过国际互联网来传播，它们或者作为电子邮件的附件，或者作为用户从国际互联网上下载的文件。[195] 这些新的、有效的传播方法大大加快了病毒的感染速度，并且大大增加了受感染计算机系统的数量。据估计，计算机蠕虫 SQL Slammer [196] 在其传播过程的最初 10 分钟内，可感染 90%的易受攻击计算机系统。[197] 仅 2000 年一年，因计算机病毒攻击而造成的经济损失估计在 170 亿美元左右。[198] 2003 年，这一数据仍然超过 120 亿美元。[199]

---

[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.

大多数第一代计算机病毒或者删除信息，或者显示消息（参见图 4）。最近，有效载荷已经变得多样化。[200] 现代的计算机病毒能够安装后门，使得攻击者可以遥控受害者的计算机或者对文件进行加密，使得受害者无法访问其自身的文件，直到他们付钱买到密钥。[201]

2.4.5 系统干扰

与针对计算机数据的攻击相比，针对计算机系统的攻击同样令人担心。越来越多的企业将国际互联网服务整合到它们的生产过程中，原因是这种服务具有每天 24 小时可用以及全球可访问的优越性。[202] 如果攻击者成功阻止计算机系统平稳运行，那么将导致受害者遭受巨大的经济损失。[203]

攻击可以通过计算机系统上的物理攻击来执行。[204] 如果攻击者能够访问计算机系统，那么他们就能够破坏硬件。对大多数刑法体系而言，远程的物理攻击并不会引发大问题，原因是它们类似有关财产破坏或损坏的典型案例。不过，对利润极高的电子商务业务而言，对计算机系统实施攻击而造成的损失，常常会比仅仅破坏计算机硬件而造成的损失大得多。[205]

对法律体系而言，更大的挑战是基于互联网的诡计。这些针对计算机系统的远程攻击的例子包括：

- 计算机蠕虫；[206] 或者
- 拒绝服务（DoS）攻击。[207]

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

[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.

计算机蠕虫[208]是恶意软件的一个子群（与计算机病毒一样）。计算机蠕虫是一种自我复制的计算机程序，它们通过启动多个数据传输过程来对网络造成损害。它们可以通过以下主要方式来影响计算机系统：

- 取决于计算机蠕虫的有效载荷，感染后的计算机系统可能停止平稳运行，并且使用系统资源在国际互联网上对自身进行复制；
- 产生网络流量，使某些服务（如网站）不再可用。

尽管计算机蠕虫的目标通常是影响整个网络，而不是针对某些特定的计算机系统，但拒绝服务（DoS）攻击的目标是一些特定的计算机系统。拒绝服务攻击使目标用户无法使用计算机资源。[209]通过发出比计算机系统能处理的请求更多的请求来攻击某个目标计算机系统（参见图 5），攻击者可以阻止用户访问计算机系统、查看电子邮件、阅读新闻、预订航班或者下载文件。2000 年，在短时间内，对一些知名的公司，如美国有线新闻网（CNN）、易趣（eBay）和亚马逊（Amazon），发动了若干次拒绝服务攻击。[210]结果是，有些服务在数小时内甚至几天内无法使用。[211]

对拒绝服务攻击和计算机蠕虫攻击进行起诉，对大多数刑法体系提出了严峻挑战，原因是这些攻击可能不会对计算机系统造成任何物理影响。除了对基于互联网的攻击需要进行定罪的基本需求外，[212]对防止和起诉针对关键基础设施的攻击是否需要一个独立的法律方法的问题，目前正在讨论中。

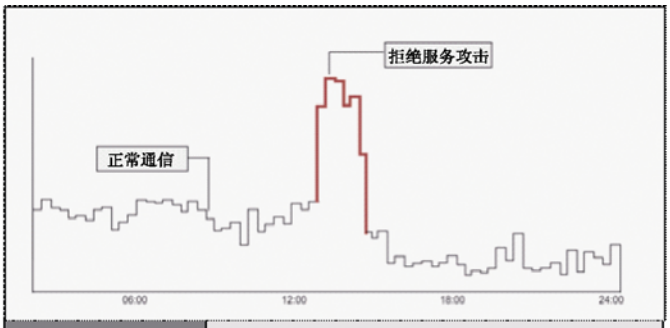


图5

图形显示在正常工作（黑）和拒绝服务（DoS）攻击期间某个网站的访问请求数量。如果被攻击的服务器无法处理增长的服务请求，那么攻击将使网站的响应速度下降或使服务根本无法提供。

[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.

[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.

2.5 内容相关的违法行为

这一类别涵盖了那些被认为是非法的内容，包括儿童色情、排外材料或者与宗教符号有关的侮辱。[213] 应对这一类别违反行为的法律手段的制定更大程度上受国家级措施的影响，需要考虑基本的文化和法律原则。对非法内容，不同社会之间的价值体系和法律体系会存在众多不同之处。在许多欧洲国家，散发排外材料是非法的，[214] 但在美国，[215] 却受到该国言论自由原则的保护。[216] 在许多阿拉伯国家，对神圣的先知使用不敬的言论是犯罪行为，[217] 但在一些欧洲国家却不是这样。

这些法律挑战是复杂的，原因是在某个国家中计算机用户可用的信息，几乎可以被全世界任何地方的人访问到。[218] 如果“攻击者”制造了在某些国家被视为非法的内容，但他身处这些国家之外，那么很难、甚至不可能起诉“攻击者”。[219]

关于材料的内容，以及特定行为应定位为何种程度的罪行，各国间很难达成一致。不同的国家观点，以及难以起诉在调查国之外的地方所犯的违法行为，已促使对国际互联网上的某些类型内容进行阻断。有些国家已就防止访问含有非法内容、主机设在国外的网站达成一致，这样，这些国家就可实施严格的法律，阻断对网站的访问，并对内容进行过滤。[220]

---

[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.

[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.

内容过滤系统可采用各种各样的方法。一种解决方案要求访问提供商安装对即将访问的网站进行分析的程序，并阻止对黑名单上网站的访问。[221] 另一种解决方案是在用户计算机上安装过滤软件（对于那些希望控制子女们网上浏览内容的父母，这是一种有用的方法，对于图书馆和公共国际互联网终端也是如此）。[222]

尝试控制国际互联网上的内容不限于那些被广泛认为是非法的内容类型。一些国家使用过滤技术来限制对涉及政治主题的网站的访问。开放网络倡议[223] 报告说，当前约有 24 个国家实施这种审查制度。[224]

2.5.1 色情材料（不包括儿童色情）

涉及色情的内容是最先通过国际互联网进行商业传播的内容之一，它为色情和淫秽材料的零售商提供了优势，包括：

- 媒介交换（如图片、视频、实况转播等），而无需进行高成本的运输；[225]
- 在世界范围内[226] 访问，客户数量可以比零售店的顾客数量多得多；
- 国际互联网常常被视为一种匿名媒介（常常是错误的[227]） — 鉴于当前主流的社会观念，这是色情内容欣赏的一个方面。

最近的研究已确定，任何时候，国际互联网上都有 420 万个色情网站可供访问。[228] 除了这些网站，色情材料还可以通过以下方式进行传播：

---

[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 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.

- 使用文件共享系统进行交流；[229]
- 在封闭的聊天室中进行交流。

不同国家对色情与淫秽材料的定罪程度各不相同。有些国家允许成年人交流色情材料，并仅对未成年人访问这类材料的情形予以定罪[230]，旨在保护未成年人。[231]研究表明，儿童接触色情内容会对其成长产生负面影响。[232]遵守这些法律，一些国家研发了“成人验证系统”（参见图 6）。[233]另一些国家则对所有有关色情材料的交流定位有罪，即使是成年人也不例外，[234]而不专门针对特定群体（如未成年人）。

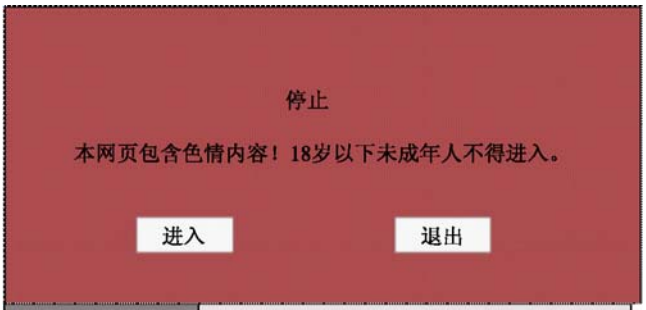


图6

图形显示了一种用于阻止未成年人访问带有色情内容网站的方法。由于该解决方案不对用户提供的答复进行验证，因此在许多国家它被认为是不合适的。

对那些对色情材料交换进行定罪的国家而言，防止访问色情材料是一个挑战。除了国际互联网，主管部门常常对违反传播色情材料禁令的行为进行侦查和起诉。不过，在国际互联网上，由于色情材料常常可以方便地在国外的服务器上获得，因此难以执法。即使主管部门能够确定那些包含色情材料的网站，它们也可能没有任何权力来强制要求提供商删去无礼的内容。

国家主权原则通常不允许某个国家在未经当地主管部门许可的条件下，到他国范围内开展调查。[235]即使当主管部门寻求违法网站托管服务国的支持时，案件的成功调查和刑事制裁也可能受到“双重犯罪”原则的阻碍。[236]为防止人们访问色情内容，制定了严格法律的国家也常常局限于防止（如采用过滤技术[237]）对某些网站的访问。[238]

---

[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.

[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

2.5.2 儿童色情

与各国对成人色情的不同观点相反，全世界都对涉及儿童色情的行为予以谴责，并将涉及儿童色情的违法行为广泛地视为犯罪行为。[239] 一些国际组织致力于与在线儿童色情作斗争，[240] 这方面的一些国际法律倡议包括：1989 年《联合国关于儿童权利的公约》[241]；2003 年《欧洲理事会关于与儿童性侵犯和儿童色情作斗争的框架决定》[242]；以及 2007 年《欧洲理事会关于保护儿童免受性侵犯和性虐待的公约》，等等。[243]

令人遗憾的是，这些旨在控制网络传播色情的倡议并没有阻止违法者通过国际互联网来传递和交换儿童色情材料（参见图 7）。[244] 带宽的增加还为此类电影和图片资料的传播与交换提供了支持。

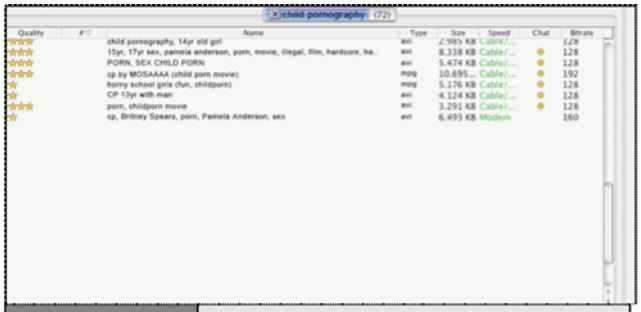


图7

图形显示的是与文件共享软件的用户接口。提交有关“儿童色情”这一术语的请求后，软件列出文件共享系统用户可用的、包含“儿童色情”这一术语的所有文件。

对涉及儿童色情的违法者行为进行的研究表明，在因涉嫌与国际互联网有关的儿童色情犯罪而逮捕的人中，15%的人在其计算机中存有 1000 多张儿童色情图片；80%的人在其计算机中存有 6～12 岁儿童的色情图片；[245] 19%的人存有年龄在 3 岁以下儿童的色情图片；[246] 21%的人存有描绘暴虐的图片。[247]

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.

[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.

销售儿童色情有大利可图，[248] 收集者愿意为描述儿童色情内容的电影和图片支付大笔费用。[249] 搜索引擎可以迅速找到此类材料。[250] 大部分材料是在有密码保护的、封闭的论坛中进行交易的，此类论坛对普通用户和执法机构而言是难以访问的。因此，暗中进行侦查是与儿童色情犯罪活动进行斗争的关键所在。[251]

在使用信息通信技术进行儿童色情材料交易中，有两个主要因素使这些罪行难以被调查：

1．使用虚拟货币和匿名支付手段 [252]：

现金支付使购买者能不暴露其身份而购得东西，因此，现金支付在许多犯罪行业中只有主导地位。对匿名支付的需求使得虚拟支付系统和实现匿名支付的虚拟货币应运而生。[253] 虚拟货币无需身份和验证，防止了执法机构对流向违法者的资金流进行跟踪。最近，大量的、对儿童色情犯罪活动的调查，成功地利用了在支付时留下的踪迹来鉴别违法者。[254] 不过，当违法者使用匿名支付时，则难以对其进行跟踪。

2．使用加密技术 [255]：

越来越多的违法者对其消息进行加密。执法机构注意到，违法者使用加密技术来保护存储在其硬盘上的信息，[256] 这严重阻碍了犯罪调查。[257]

除了对涉及儿童色情的犯罪行为进行广泛定罪外，目前正在讨论其他一些方法，如履行国际互联网服务必须注册用户的义务，或者阻止或过滤对涉及儿童色情内容的网站的访问等。[258]

---

[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.
[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.

2.5.3 种族主义、仇恨言论、鼓吹暴力

激进团体使用国际互联网等大众传播系统来开展宣传活动（如图 8 所示）。[259] 最近，提供种族主义内容和仇恨言论的网站数量已经在增长[260] — 2005 年的一份研究表明，在 2004 年至 2005 年间，鼓吹种族仇恨、暴力和排外主义的网页数量增加了 25%。[261] 2006 年，在国际互联网上存在 6000 多个类似的网站[262]。

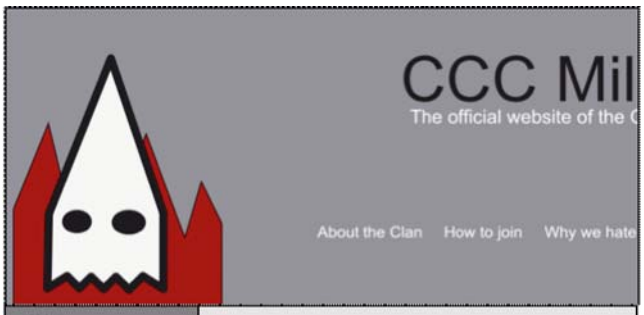


图8

图形显示的是一个激进团体的网站。此类团体对国际互联网用得很多，用来向公众宣告其目标，并用来招募新成员。

国际互联网的传播为违法者提供了若干优势，包括更低的传播成本、无需专业设备以及在全球范围内散布。鼓吹仇恨网站的例子包括介绍如何制造炸弹的网站。[263] 除了进行宣传活动之外，国际互联网还被用来出售某些产品，如与纳粹有关的物品，包括带纳粹符号的旗帜、制服和书籍，这些东西都可以在拍卖平台和专门的互联网商店中轻易地得到。[264] 国际互联网还用来发送电子邮件、新闻简报，以及传播视频片段和电视节目，方法是通过一些受欢迎的网站，如 YouTube。

并非所有国家都对这些违法行为定罪。[265] 在有些国家，此类内容可能得到言论自由原则的保护。[266] 对某些主题言论自由原则运用到何种程度，各国之间存在不同意见，这常常妨碍了国际调查。这方面法律冲突的一个例子涉及国际互联网服务提供商雅虎。2001 年，法国的一个法庭命令雅虎（位于美国）阻止法国用户访问与纳粹有关的内容。[267] 根据美国宪法第一修正案，销售此类材料并不违反美国法律。根据第一修正案，美国的一个法庭宣布法国的命令无法对位于美国的雅虎执行。[268]

---

[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.
[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.

在起草《欧盟理事会关于网络犯罪的公约》时，各国之间对这些问题的分歧表现明显。《公约》寻求协调与网络犯罪有关的法律，以确保国际调查不因法律冲突而受阻。[269] 在讨论关于如何就散布排外主义材料的行为定罪时，并非参加谈判的所有各方都一致同意，因此，这整个主题排除在了《公约》之外，取而代之的是在一个单独的《第一协议》中进行了论述。[270] 否则，有些国家（包括美国在内）可能不会签署《公约》。

2.5.4 宗教违法行为

越来越多的网站[271]介绍一些其他国家可能视为冒犯宗教的行为内容，如反宗教的书面声明。[272] 尽管有些材料记录了客观的事实与趋势（如欧洲参加教堂活动的人数日益减少），但在一些管辖区域中，这类信息也可能被视为非法。另一些例子包括诽谤宗教或者出版漫画（图 9）。

图9

图形显示的是一个带有宗教背景的网站，可供世界范围内的用户访问。

国际互联网为那些希望引起争论或对某一主题进行批判的人提供了优势 — 人们可以留下评论、张贴内容或者撰写文章，而不必暴露其身份。许多辩论团体都是基于言论自由原则的。[273] 言论自由原则也是国际互联网成功背后的一个主要推动因素，门户网站是专用于用户自己制作的内容的。[274] 虽然保护这一原则至关重要，但即使在最自由的国家，言论自由原则的适用也受到各种条件和法律的控制。

关于非法内容的不同法律标准，体现了在管理这些内容中所面临的挑战。尽管在那些奉行言论自由原则的国家可以发表某些内容，但在另一些管制更严格的国家，它可能会受到指责和控告。2005 年的“漫画争议”就显示了各国法律冲突的可能性。一家丹麦报纸《日德兰邮报》发表的十二幅由编辑制作的漫画，引发了穆斯林世界的广泛而强烈的抗议。[275]

---

[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.

谈到非法内容，在某些国家，提供某些信息或材料的可用性是一种犯罪行为。国与国之间对不同宗教信仰和宗教符号的保护政策各不相同。有些国家对“圣洁先知”[276]使用不敬言论或者玷污《可兰经》[277]的行为认为有罪，而另一些国家则可能采取更为自由的方法，可能不对此类行为进行定罪。

2.5.5 非法赌博与在线游戏

国际互联网游戏和网络赌博是国际互联网世界里增长最快的领域之一。[278]在线游戏“Second Life”的研发商林登（Linden）实验室[279]报告说，该游戏目前大约有 1000 万注册用户。[280]有报告显示，一些此类游戏已被用来实施犯罪，包括：[281]

- 儿童色情内容的交换和展示；[282]
- 欺诈；[283]
- 在线赌场中的赌博；[284]以及
- 诽谤（例如，留下诽谤性或损害他人名誉的消息）。

有人估计，从 2001 年到 2010 年的 10 年间，预计国际互联网在线赌博的年均收入从 31 亿美元增长到了 240 亿美元[285]（尽管与传统赌博业的收入相比，这些估计值仍然相对较小[286]）。

[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;

各国对国际互联网上和国际互联网外的赌博的管制各不相同[287] — 这正是违法者、合法企业以及各个赌场加以充分利用的一个漏洞。不同管制的效应在澳门最为明显。自从 1999 年澳门从葡萄牙回归中国后，澳门已经成为全世界最大的赌博目的地之一。2006 年，澳门赌博业估计的年收入为 68 亿美元，取代了拉斯维加斯的龙头老大位置（拉斯维加斯的赌博业年收入为 66 亿美元）。[288] 澳门的成功源于中国法律禁止赌博这一事实，[289] 每年有成千上万的大陆居民前往澳门赌博。

国际互联网使人们可以绕过对赌博的限制。[290] 在线赌场在网上随处可见（参见图 10），而大多数的托管服务机都设在对国际互联网赌博不加限制或者法律宽松的国家。用户可以在线开设账号，转移资金并且玩这种运气游戏。[291] 在线赌场还可以用于洗钱和资助恐怖主义等活动。[292] 如果违法者在不保存记录的下注阶段使用在线赌场，或者在没有针对洗钱犯罪进行过立法的国家中使用在线赌场，那么执法机构将难以确定资金的源头。

图10

图形显示的是一个在线娱乐场的用户接口。注册和兑换货币后，用户即可参与在线赌博。许多在线娱乐场无需正式注册过程即可享受服务。

对于那些限制赌博的国家，难以控制人们对在线赌场的使用或参与在线赌博活动。国际互联网破坏了一些国家禁止公民参与在线赌博的法律限制。[293] 一些国家试图通过立法防止国民参与在线赌博：[294] 一个著名的例子是，美国于 2006 年出台的禁止国际互联网赌博法案，它试图通过对那些涉及非法赌博结算的金融服务提供商进行起诉来限制非法的在线赌博。[295]

[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.

[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.

2.5.6 诽谤与虚假信息

国际互联网可用来散布虚假信息，这与用它来发布真实信息一样容易。[296] 网站可以发布虚假的或诽谤性的信息，尤其是在论坛和聊天室中，在这些地方，用户可以不经过版主的验证就可发布消息。[297] 越来越多的未成年人使用网上论坛和社会网站，而在这些地方也可以发布类似的虚假或诽谤信息。[298] 犯罪行为 [299] 包括（例如）发布激情照片或者发布关于性行为的虚假信息。[300]

在大多数情况下，违法者利用以下事实来实施犯罪活动，即提供商可以廉价或免费发布消息，通常无需发布者身份证明或者不必验证身份。[301] 这使得对违法者的身份识别变得更加复杂。此外，论坛版主对其中发布的内容不做规定，或者只有很少的规定（图 11）。但这些优势并没有阻碍到一些有价值项目的发展，如由用户生成的在线百科全书 — 维基（Wikipedia）[302]，该项目对发布的内容存在严格的管制程序。不过，违法者也可以使用同样的技术来：

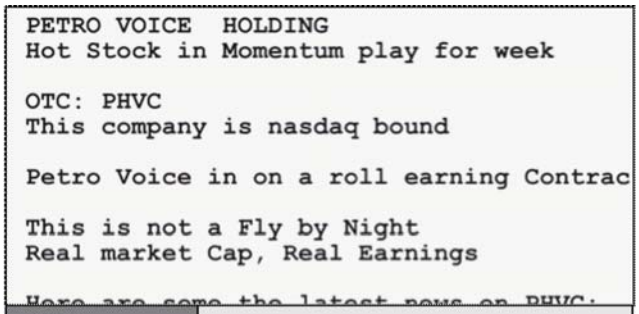


图11

垃圾邮件是一个严重的问题。这些电子邮件涉及众多主题。除了推销不同的产品之外，提供有关股票的信息也很普遍。

- 发布虚假信息（例如，发布关于竞争者的虚假信息）；[303]
- 诽谤（例如，留下诽谤性或损害他人名誉的消息）；[304]
- 泄露秘密消息（例如，发布国家机密或者敏感的商业情报）。

[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.
[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.

重要的是强调虚假或欺骗信息所带来的日益严重的威胁。诽谤可以在很大程度上严重毁坏受害者的名誉和声望，原因是全球的用户都可以访问到在线信息。从信息在国际互联网上发布的那一刻起，作者往往就失去了对它的控制。即使在信息发布后不久就更正或删去，它也可能已被复制（“镜像”），并被那些不愿撤销或删除它的人得到。在这种情况下，信息在国际互联网上仍然是可用的，即使最初的发布者已经删除或者更正了它。[305] 这方面的例子包括“失去控制的电子邮件”，数以百万计的用户可以接收到关于个人或组织的色情的、欺骗的或虚假的电子邮件，而它们对名誉的伤害也许永远无法消除，尽管事实与最初发出的电子邮件完全相反。因此，需要在言论自由[306]与保护因言论自由而可能遭到伤害的受害者之间保持良好的平衡。[307]

2.5.7 垃圾信息与相关威胁

“垃圾邮件”指的是发送主动提供的大量消息（图 12）。[308] 尽管存在各种各样的垃圾信息，但最为常见的是垃圾邮件。违法者向用户发出数百万封电子邮件，常常包含产品和服务的广告，但也经常带有一些恶意软件。自从 1978 年第一封垃圾邮件发出之日起，[309] 垃圾邮件便呈现急剧增长的态势。[310] 如今，根据电子邮件提供商组织的报告，在所有电子邮件中，多达 85%～90%是垃圾邮件。[311] 2007 年，垃圾邮件主要来自：美国（占记录总数的 19.6%）；中华人民共和国（占记录总数的 8.4%）以及韩国（占记录总数的 6.5%）。[312]

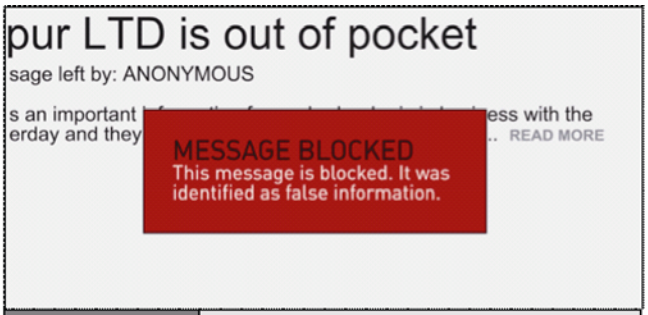


图12

在无需正式注册即可留言的国际互联网论坛上发布含有虚假内容的消息是很普遍的。

[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.

[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.

大多数电子邮件提供商对垃圾邮件数量猛增的态势作出了反应，方法是采用饭垃圾邮件过滤技术。这种技术使用关键字过滤器或者垃圾邮件发送者 IP 地址黑名单来识别垃圾邮件。[313] 尽管过滤技术仍在继续研发之中，但垃圾邮件发送者已经围绕这些系统在寻找应对之策 — 例如，避开过滤技术可能发现的关键字。垃圾邮件发送者已经找到许多办法来描述“伟哥”这种最常出现在垃圾邮件中的产品，方法是在电子邮件中不使用其商标名称。[314]

成功检测垃圾邮件取决于垃圾邮件传播方式是否改变。许多攻击者不是使用单个邮件服务器来发送垃圾邮件（由于其源头数量有限，[315] 这在技术上更易于检测到垃圾邮件提供商），而是运用僵尸网络 [316] 来分发主动提供的电子邮件。通过使用基于成千上万个计算机系统的僵尸网络，[317] 每台计算机可能只发送几百封电子邮件。这使电子邮件提供商更难借助分析邮件发送者信息的方法来识别垃圾邮件，也使执法机构更难追踪攻击者。

由于发送数十亿封垃圾邮件的成本很低，因此垃圾邮件是十分有利可图的 — 如果使用僵尸网络，那么成本更低。[318] 有些专家建议，在与垃圾邮件作斗争的过程中，唯一真正的解决方案是提高发送者的邮件发送成本。[319] 2007 年公布的一份报告对垃圾邮件的成本与利润进行了分析。根据分析结果，发送 2000 万封垃圾邮件的成本约为 500 美元。[320] 由于发送者成本很低，因此发送垃圾邮件的利润相当高，尤其当发送者能够发送数十亿封电子邮件时。荷兰的一位垃圾邮件发送者指出，通过发送至少 90 亿封垃圾电子邮件，它获得了大约 50000 美元的利润。[321]

2005 年，经济合作与发展组织公布了一份报告，对垃圾邮件对发展中国家的影响进行了分析。[322] 发展中国家常常表达这样的观点：它们国家中的国际互联网用户更多地受到垃圾邮件和国际互联网滥用的影响。垃圾邮件在发展中国家里是一个严重问题，原因是在发展中国家，带宽和国际互联网接入资源比在工业化国家更稀缺、更昂贵。[323] 在那些国际互联网资源更稀缺、更昂贵的国家，垃圾邮件占用了宝贵的时间与资源。

---

[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.

[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

2.5.8 其他形式的非法内容

国际互联网不仅用于直接攻击，而且还可作为一个论坛，进行以下非法活动：

- 教唆犯罪、煽动犯罪；[324]
- 非法出售产品；以及
- 为非法行为提供信息和指导（例如，指导如何制造爆炸物）。

许多国家对某些产品的交易实施严格的管理。不同国家运用不同的国家规定和贸易限制来对各种产品进行严格的监管，如军用装备。[325] 药品也面临同样的情形 — 在某些国家不受限制即可获得的药品，在另一些国家可能需要处方。[326] 跨境贸易使得难以确保对某些产品实施严格限制。[327] 鉴于国际互联网的广泛普及，这一问题变得更为严重了。在那些不设限制的国家中经营的互联网商店，可以向其他设有严格限制的国家的客户出售产品，这就破坏了这些限制。

在国际互联网问世之前，大多数的人难以接触到如何制造武器之类的指南。尽管也可以获得一些必要的信息（例如，在涉及爆炸物方面化学的书籍中），但这相当费时。如今，国际互联网上就有关于如何制造爆炸物的指南，[328] 而且可以轻易地获得此类信息，这增大了攻击的可能性。

2.6 与版权和商标有关的违法行为

图13

图形显示了第二代文件共享系统的功能。第一代文件共享系统基于集中式服务器，作为可用文档清单的宿主机。在第二代文件共享系统中，服务器的功能委托给用户，使之更难以对网络造成影响，并防止出现版权冲突问题。

国际互联网至关重要的功能之一是传播信息。各家公司使用国际互联网来传播关于其产品与服务的信息。在盗版方面，成功的公司在国际互联网上可能面临的问题，比那些网络之外存在的问题有过之而无不及。它们的品牌形象和公司设计可能用于推销仿造的产品，而仿造者复制公司的标识，仿造其产品，并试图在与该公司相关的域上注册。直接通过国际互联网发售其产品的公司 [329] 可能面临与侵犯版权有关的法律问题。它们的产品可以被下载、复制和发售。

---

[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/imguploa d/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.
[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.

2.6.1 与版权有关的违法行为

利用数模转换，[330] 数字化 [331] 使得娱乐行业为 DVD 中的电影增加了额外的特点与服务，包括语言、副标题、预告片以及额外赠送的材料。CD 和 DVD 已被证明能比录音带和录像带保存更长的时间。[332]

数字化也为新的版权侵犯行为打开了方便之门。当前侵犯版权的基础是快速而准确地复制。在数字化之前，复制一盘录音带或录像带总会导致一定程度的质量下降。如今，复制数字音像制品几乎不会造成质量的下降，因此，也能够从任何拷贝再次复制。最常见的版权侵犯行为包括：

- 在文件共享系统中共享受版权保护的歌曲、文件和软件；[333]
- 避开数字版权管理系统。[334]

文件共享系统是基于点对点 [335] 的网络服务，它使用户能够共享文件，[336] 常常可以与数百万个其他用户实现共享。[337] 在安装文件共享软件后，用户可以选择一些文件来共享，并使用软件来搜索其他可用的文件，这些文件可从数百个出处下载。在文件共享系统问世之前，人们需要复制录音带和录像带，然后才能进行交换，文件共享系统则允许更多的用户进行拷贝交换。

点对点（P2P）技术在国际互联网中起着至关重要的作用。当前，超过一半的用户国际互联网通信流量是由点对点网络产生的。[338] 用户数量一直在增长 — 经济合作与发展组织公布的一份报告估计，30%左右的法国国际互联网用户在文件共享系统中下载过音乐或文件，[339] 而这一组织中的其他国家也呈现类似的趋势。[340] 文件共享系统可用来交换任何类型的计算机数据，包括音乐、电影和软件。[341] 过去，文件交换系统主要用来交换音乐，但如今，视频材料的交换变得愈来愈重要了。[342]

---

[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.

[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.

用于文件共享服务的技术极为先进，能够在短时间内交换大型文件。[343] 第一代文件共享共享依靠一台中央服务器，使得执法机构能够针对 Napster 网络中的非法文件共享行为采取行动。[344] 与第一代系统（尤其是著名的服务 Napster）不同，第二代文件共享系统不再以中央处理器为基础（中央处理器用于提供用户间可用的文件列表）。[345] 第二代文件共享系统的分散管理概念（参见图 13），使得更难以防止它们运行。不过，由于采用直接通信，因此，通过用户的 IP 地址，还是有可能跟踪到网络用户的。[346] 执法机构已经在调查文件共享系统中的版权侵权问题上取得一些成功。最近版本的文件共享系统能够实现多种形式的匿名通信，这将使版权侵权问题的调查变得更加困难。[347]

文件共享技术不仅可被普通用户和犯罪分子使用，普通的企业也可以使用。[348] 并非在文件共享系统中交换的所有文件都侵犯版权。合法使用文件共享系统的例子包括授权拷贝的交换或者公共域中的艺术作品。[349]

尽管这样，文件共享系统的使用仍然对娱乐行业提出了挑战。[350] 目前尚不明确，CD/DVD 以及电影票销量的下滑究竟在多大程度上应归咎于文件共享系统中电影拷贝的交换。研究确定已有数百万个文件共享用户 [351] 以及数十亿个已被下载的文件。[352] 常常是在电影在电影院正式上映之前，电影拷贝就已经出现在文件共享系统中，[353] 这损害了版权持有者的利益。匿名文件共享系统的最新发展将使版权持有者的反盗版工作更难进行，也令执法机构更难执法。[354]

---

[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; *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.

通过实施一种专用于防止用户制造 CD 和 DVD 拷贝的技术，如内容加扰系统（CSS）[355] — 一种旨在防止 DVD 上内容被拷贝的加密技术，[356] 娱乐业已经对盗版行为作出了反应。这种技术是新商业模式一个不可或缺的因素，旨在更加准确地向用户赋予访问权限。数字版权管理（DRM）[357] 描述了有关技术的实施情况，它们允许版权持有者限制他人对数字媒体的使用，客户只能购买有限的权限（例如，只能在一次集会上演唱某首歌曲的权限）。数字版权管理使得新商业模式的实施成为可能，它可更加准确地体现版权持有者和用户的权益，有望扭转利润下滑的趋势。

这些技术最大的困难之一是，侵权者可以绕过版权保护技术。[358] 侵权者已经开发出一些软件工具，使软件工具用户能够使受版权保护的文件在国际互联网上可用，[359] 且是免费的，或者价格低廉。一旦从文件中移去数字版权管理（DRM）保护措施，拷贝就可以不受限制地被复制和使用。

版权保护的内容不只限于歌曲和电影。有些电视台（尤其是付费电视频道）对其节目进行加密，以确保只有付费用户才能收看到节目。尽管此类保护技术十分先进，但违法者仍成功地使用软件工具伪造了用于访问控制的硬件，或者破解了密码。[360]

没有软件工具，普通用户不太可能实施违法行为。对侵犯版权行为的定罪的讨论，不仅关注文件共享系统和绕过技术保护，而且关注生产、销售和拥有旨在使用户能够实施版权侵权活动的“非法设备”或工具。[361]

2.6.2 与商标有关的违法行为

侵犯商标类似于侵犯版权，也是全球贸易中一个广为人知的问题。涉及商标的侵犯行为已经转向网络空间，根据不同国家的刑法，定罪的轻重也各不相同。[362] 最严重的违法行为包括：

- 在犯罪活动中使用商标误导目标对象；以及
- 与域名或名称有关的违法行为。

[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.
[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;

一家公司的良好声誉常常直接和其商标相关联。违法者在许多活动中使用品牌名称和商标进行欺诈，包括“网络钓鱼”（参见图 14），[363] 在此类违法行为中，违法者向国际互联网用户发出数百万封电子邮件，这些邮件与合法公司发出的电子邮件相似，例如，都包括其商标。[364]

与商标侵权有关的另一个问题是与域名有关的违法行为，[365] 如域名抢注，[366] 是指注册一个与某一产品或某家公司的商标相同或相似的域名的非法行为。[367] 在大多数情况下，违法者寻求向该公司高价出售这一域名，[368] 或者利用它来销售产品或服务，借助用户对该商标信以为真的连接来误导他们。[369] 另一种与域名有关的违法行为是“域名劫持”或者注册偶然终止的域名。[370]

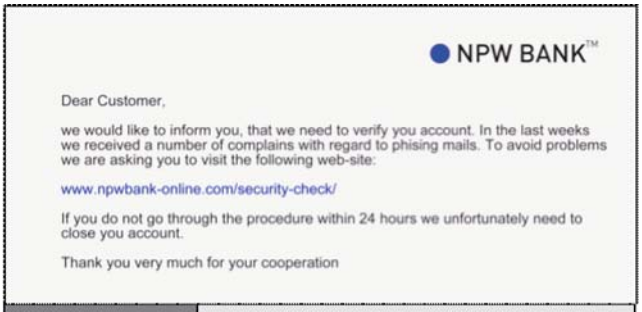


图14

图形显示的是一个网络钓鱼邮件。设计的网络钓鱼邮件模仿来自合法公司的通信。攻击者常常使用原版的、受商标法保护的标识。

2.7 与计算机有关的违法行为

这一类别涵盖大量的违法行为，它们需要借助计算机系统来实施。与之前的类别不同，这些众多的违法行为通常不会受到法律原则的严格保护，它们包括：

- 与计算机有关的欺骗；
- 与计算机有关的伪造、网络钓鱼和身份盗用；以及
- 设备误用。

[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.

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

2.7.1 欺骗和与计算机有关的欺骗

与计算机有关的欺骗是国际互联网上最常见的犯罪之一，[371] 原因是它使违法者能够使用自动操作工具 [372] 和软件工具来掩盖作案者的身份。

自动操作工具可使违法者从大量的小金额违法行为中获取巨额利润。[373] 违法者使用的一种策略是确保每个受害者遭受的经济损失都低于某个特定界限。由于损失“很小”，受害者不太可能耗费时间和精力来报告和调查此类罪行。[374] 此类骗局的一个例子是尼日利亚的预付金欺诈案（参见图 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.

图15

图形显示的是一个典型的、基于预付费欺骗诡计的电子邮件。为了获得设想的利润，要求邮件接收者预先转一部分账。这是一个非常流行的欺骗诡计，但由于没有计算机系统的处理，因此它不是一种与计算机有关的欺骗。

尽管这些违法行为都是使用计算机技术来实施的，但大多数刑法体系并未将其归类为与计算机有关的违法行为，而是将其归类为普通欺诈。[376] 与计算机有关的欺诈与普通欺诈之间的主要区别在于欺诈的对象。如果违法者试图影响一个人，那么其行为通常被视为欺诈。如果违法者以计算机或数据处理系统为目标，那么其行为通常被视为与计算机有关的欺诈。那些涵盖欺诈行为但尚纳入出于欺诈目的而操纵计算机系统的违法行为的刑法体系，常常也会对上述行为进行起诉。

最常见的欺诈骗局包括：

1. 在线拍卖欺诈 [377]

在线拍卖目前是最受欢迎的电子商务服务之一。2006 年，通过易趣（eBay）销售的商品价值超过 200 亿美元，使得易趣（eBay）成为世界上最大的在线拍卖市场。[378] 购买者可以从世界各地通过国际互联网访问各种不同的或者专门的商品。销售者乐于面对全球受众，刺激需求、提升价格。

---

[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.
[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/Falooutsos*, 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.

通过拍卖平台实施犯罪的违法者，可以充分利用买方与卖方之间不存在面对面签订合同的机会。[379] 由于难以区别真正的用户与违法者，因此导致拍卖欺诈成为最常见的网络犯罪之一。[380] 以下是两种最常见的骗局：[381]

- 用一种实际并不存在的商品进行销售，并要求买方在发货之前付款；[382] 或者
- 买下商品并要求发货，但不打算付款。

在应对这种违法活动时，拍卖提供商开发了一种保护系统，如反馈/评价系统。在每笔拍卖交易后，买方和卖方留下供其他用户使用的反馈意见，[383] 作为一种关于买方/卖方可靠性的中性信息。在这种情况下，“信誉就是一切”，如果没有足够数量的积极评价，违法者难以说服他要欺诈的对象为并不存在的商品付款，或者相反地，在没有预先收到付款的情况下发货。

不过，作案者也为此想出了对策，通过使用第三方的账号，来绕过这一保护措施。[384] 在这一骗局中称为“账号接管”，[385] 违法者设法掌握合法用户的用户名和密码，以便以欺诈手段购买或销售商品，使执法机构更难确定违法者的身份。

2. 预付金欺诈 [386]

在预付金欺诈中，违法者发出电子邮件，请求接收者帮助向第三方转移大笔资金，并承诺，如果接收者同意使用其个人账号来转账，那么将给其一定比例的“回扣”。[387] 然后，违法者要求邮件接收者转移一笔小额资金，以验证其银行账号数据（基于一种类似于碰碰运气的情形 — 接收到邮件的人也许愿意遭受小而肯定的损失，来换取大而不可能的收入），或者要求他们直接发送银行账号数据。一旦受害者转移了资金，他们将再也联系不上违法者。如果他们向违法者发送了银行账号信息，那么后者可能利用这些信息来进行其他欺诈活动。有证据表明，数以千计的受害者对此类电子邮件进行了回复。[388] 当前的研究表明，尽管政府部门进行了各种各样的宣传，也采取了一些举措来遏制这种犯罪，但预付金欺诈案件的数量仍在不断增长 — 不仅仅是受害者的数量在增加，总的损失数额也在增加。[389]

---

[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.

[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.

2.7.2 与计算机有关的伪造

与计算机有关的伪造指的是对数字文件的操纵[390] — 例如，通过以下三种方法：

- 创建一个看起来像来自可靠机构的文件；
- 篡改电子图像（例如，用来在法庭上作为证据的图片）；或者
- 更改文本文件。

伪造电子邮件包括“网络钓鱼”骗局，这对全世界的执法机构都是一个严峻的挑战。[391] “网络钓鱼”力图让欺诈对象泄露个人/秘密信息。[392] 通常，违法者发送看似由倍受欺诈对象依赖的合法金融机构发出的邮件。[393] 这些电子邮件在设计上使受害者难以辨别它们是伪造的电子邮件。[394] 电子邮件请求接收者透露和/或验证某些敏感信息。许多受害者上当受骗，透露了某些敏感信息，使违法者能够实施在线转账等犯罪行为。[395]

过去，对涉及与计算机有关的伪造行为的起诉十分少见，原因是大多数法律文件都是有形的文件。如今，数字文件发挥的作用愈来愈大，而且用得也更加频繁。数字文件取代传统文件得到了一些法律手段的支持，例如，通过认可数字签名的法律（参见图 16）。

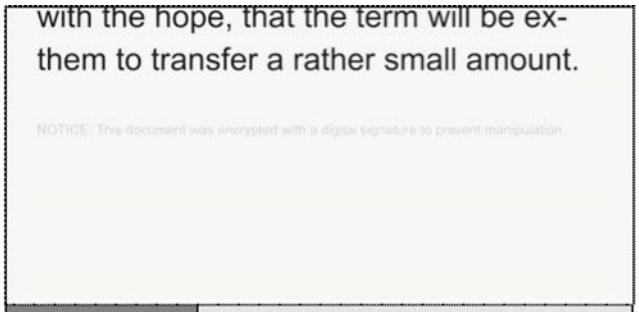


图16

相比传统的文件伪造，电子数据更易处理。技术解决方案可防止未经认可的处理，如数字签名。

作案者总是企图篡改文件。如今，利用数字伪造，可以在不降低质量的前提下拷贝数字文件，并轻易地进行篡改。对取证专家而言，难以证明数据文件是否被篡改过，除非使用技术保护措施[396] 来保护可能被篡改的文件。[397]

2.7.3 身份盗用

身份盗用这一术语既不会始终如一地定义，也不会始终如一地使用，它指的是利用欺诈手段获取和使用他人身份的犯罪行为。[398] 实施这些犯罪行为无需使用技术方法[399]，也无需使用国际互联网技术。[400]

---

[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.

[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-

一般地，被视为身份盗用的违法行为包含三个不同的步骤：[401]

- 第一步，违法者获取与身份有关的信息。例如，这一步可以通过使用恶意软件或网络钓鱼攻击来实施；
- 第二步的特点是在犯罪活动中在使用这些信息之前对与身份有关的信息进行交易。[402] 一个例子是出售与身份有关的信息。[403] 例如，信用卡记录的售价就曾高达 60 美元；[404]
- 第三步是将与身份有关的信息用于犯罪行为相。在大多数情况下，访问与身份有关的数据可使作案者能够进一步实施犯罪。[405] 因此，作案者不会着眼于数据集本身，而着眼于将它们用于实施犯罪活动的能力。此类犯罪活动的例子可以是身份识别文件伪造或信用卡欺诈。[406]

在第一步中，用来获取数据的方法涵盖许多行为。违法者可以利用物理方法，如窃取带有与身份有关数据的计算机存储设备、搜索垃圾（“垃圾搜寻”[407]）或者邮件盗窃。[408] 此外，他们可以使用搜索引擎来寻找与身份有关的数据。“谷歌黑客”或者“谷歌剁客”指的是使用复杂的搜索引擎查询来过滤大量的搜索结果，以便寻找与计算机安全问题有关的信息以及可以在身份盗用骗局中使用的个人信息。例如，作案者的其中一个目的是搜索不安全的密码保护系统，以便从中获取数据。[409] 一些报告强调指出，搜索引擎的合法使用也会伴随用于非法目的的风险。[410] 类似的问题也涉及文件共享系统。美国国会最近讨论了文件共享系统是否存在获取可被身份盗用者滥用的个人信息

---

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_cooperation/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.

[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/.

的可能性。[411] 除此之外，违法者还可以利用内部人员，后者有权访问所储存的、与身份有关的信息。美国计算机安全协会（CSI）于 2007 年开展的计算机犯罪与安全调查[412] 表明，超过 35%的回复者将其所在组织超过 20%的损失归咎于内部人员的泄密。最后，作案者可以使用社会工程技术来说服受害者泄露其个人信息。最近几年，通过采用社会工程技术来操纵受害者，作案者设计了有效的骗局来获取秘密信息（如银行账号信息和信用卡数据）（参见图 17）。[413]

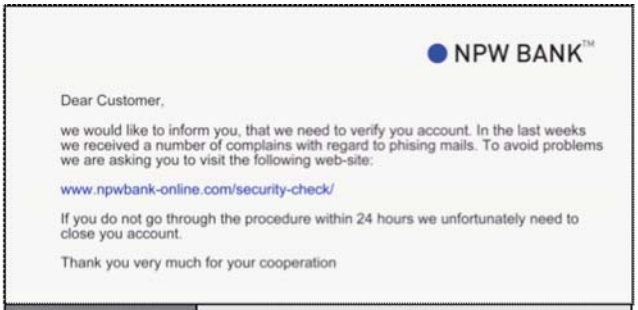


图17

网络钓鱼邮件用来从目标处获得秘密信息（如账号信息、密码和交易数据）。攻击者可利用该信息来从事违法活动。

作案者企图获取的数据类型也不是一成不变的。[414] 他们最感兴趣的数据包括：

- 社会保险号（SSN）或者护照号 — 例如，在美国，社会保险号是一种典型的、与个人身份有关的数据例子，作案者常盯着这一目标。尽管社会保险号的创建是为了保存一份准确的收入记录，但如今，它广泛用于证明某人的身份。[415] 作案者可以使用社会保险号以及获取的护照信息来开设银行账号、接管现有的银行账号、建立信誉或者迅速增加借款数额。[416]

- 生日、地址和电话号码 — 如果此类数据与其他信息（如社会保险号）[417] 相结合，那么它们一般只能用于实施身份盗用犯罪。访问到诸如生日和地址之类的额外信息，将有助于作案者绕过验证程序。与这种信息有关的最大危险之一是，它们目前在国际互联网上被广泛使用 — 或者是在各种各样与身份有关的论坛上自愿公开，[418] 或者是出于在网站上留下印记的法律要求。[419]

[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).

- 非用于银行账号的密码 — 访问到这些密码，作案者将可以改变账号的设置，使之为己所用。[420] 例如，他们可以接管一个电子邮件账号，并用来发送含有非法内容的邮件，或者接管用户在拍卖平台上使用的账号，并用该账号来销售赃物。[421]

- 用于银行账号的密码 — 与社会保险号信息一样，涉及银行账号的信息是身份窃贼常常盯着的目标，包括支票账号和储蓄账号、信用卡、借记卡、金融规划信息。对身份窃贼而言，此类信息是其实施网络金融犯罪的一个重要信息源。

身份盗用是一个严重问题，而且它的发案数量在与日俱增。[422] 最近的数据表明，2004 年上半年，3%的美国家庭感到自己成为了身份盗用的受害者。[423] 在英国，每年因身份盗用而给本国经济带来的损失高达 13 亿英镑。[424] 在澳大利亚，估计因身份盗用而带来的损失每年在不到 10 亿美元和超过 30 亿美元之间。[425] 2006 年，一次有关身份欺诈的调查估计，美国在 2005 年因身份欺诈而造成的损失高达 566 亿美元。[426] 损失不仅仅是经济上的，还包括对名誉的损害。[427] 在现实中，许多受害者并没有报告此类犯罪行为，同时金融机构也往往不希望大肆宣传客户的遭遇。身份盗用造成的真实损失可能远超出报告的损失。[428]

身份盗用基于以下事实，即国际互联网上几乎没有手段来验证用户的身份。在现实世界中识别人们的身份容易得多，而大多数形式的在线身份复杂得多。先进的身份识别工具（如使用生物测定信息）既昂贵，也尚未广泛应用。而针对在线行为的限制少之又少，因此使得身份盗用既容易，又有利可图。[429]

2.7.4 设备误用

只要使用一些基本的设备，就可以实施网络犯罪。[430] 诸如诽谤或在线欺诈等违法行为，除了一台计算机和接入国际互联网，再不需要别的设备，而且可以从某家公共的网吧来实施。更加老练和高级的违法行为则可能使用专业的软件工具来实施。

---

[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.

实施复杂违法行为所需的工具在国际互联网上唾手可得，[431] 而且常常是免费的。更高级的工具则需花费数千美元。[432] 使用这些软件工具，违法者只需按下一个按钮，便可对其他的计算机系统发动攻击（参见图 18）。如今，标准的攻击变得效率低下，原因是保护软件公司对当前可用的工具进行了分析，并对标准的黑客攻击已有所防范。引人注目的攻击通常是针对特定目标的。[433] 有些软件工具是用来进行以下违法活动的：[434]

图18

攻击者可利用许多工具来自动攻击所有使用某个预定义IP范围内IP地址的计算机系统。在此类软件帮助下，有可能在几个小时内对几百个计算机系统实施攻击。

- 实施拒绝服务攻击；[435]
- 设计计算机病毒；
- 对加密的通信进行解密；以及
- 非法访问计算机系统。

目前，第二代软件工具可以自动执行许多网络骗局，并且能够使违法者在短时间内进行多次攻击。软件工具还可以简化攻击，使经验不足的计算机用户也能实施网络犯罪。垃圾邮件工具套件唾手可得，几乎使任何人都能发送垃圾电子邮件。[436] 如今，软件工具还可用来向文件系统上载文件或从中下载文件。由于专门设计的软件工具的可用性日益增大，潜在攻击者的数量已经急剧增多。不同国家以及国际社会正在采取一些立法措施来遏制网络骗局软件工具的增长势头，例如，通过对生产、销售或拥有这些工具的行为进行定罪。[437]

2.8 组合违法行为

有许多术语可用来描述包含众多不同违法行为的复合阴谋。例子包括：

- 网络恐怖主义
- 网络洗钱；以及
- 网络钓鱼。

[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.

2.8.1 网络恐怖主义

回溯到 20 世纪 90 年代，关于恐怖组织对网络使用的讨论着重于对关键基础设施发动基于网络的攻击，如交通和能源供应设施（“网络恐怖主义”）以及在武装冲突中使用信息技术（“网络战争”）。[438] 病毒和僵尸网络攻击的成功，清楚地展现了网络安全中的薄弱环节。恐怖分子成功地进行基于国际互联网的攻击是可能的，[439] 但难以评估这种威胁的严重性，[440] 另外，相比当前的发展状况，当时的互联程度较低，这很有可能是此类事件很少见诸报端的主要原因之一，当然，有些国家出于利益考虑对成功的攻击保守秘密也是原因之一。因此，至少在过去，被风吹倒的树对电力供应造成的威胁，要比成功的黑客攻击造成的威胁大。[441]

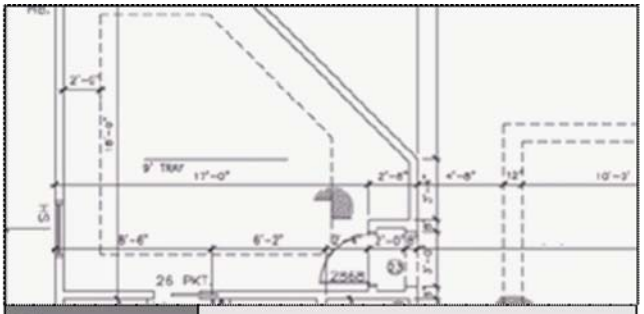


图19

国际互联网是一个重要的信息源，包括有关要寻找的潜在目标（如公共建筑物）的信息（如结构规划），例如，建筑师网站等。

但在 9·11 袭击之后，这种状况发生了改变。人们开始大量讨论恐怖分子使用信息通信技术进行破坏的问题。[442] 有报告指出，[443] 恐怖分子在准备攻击的过程中使用了国际互联网[444]，更加推动了这种讨论。尽管这些攻击不是网络攻击，实施 9/11 袭击的恐怖分子并没有实施基于国际互联网的攻击，但国际互联网在攻击的准备阶段起到了重要作用。[445] 在这一背景中，恐怖组织使用国际互联网的各种不同方法开始浮出水面。[446] 如今，众所周知，恐怖分子利用信息通信技术和国际互联网来进行以下违法活动：

---

[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.;

- 进行宣传活动；
- 收集信息；
- 准备在现实世界实施攻击；
- 发布培训材料；
- 通信；
- 恐怖分子筹集资金；
- 对关键基础设施发动攻击。

讨论焦点的这种转变，对与网络恐怖主义有关的研究产生了积极影响，原因是它突出了此前人们不知道的恐怖活动范围。但尽管综合治理方法相当重要，对关键基础设施发动基于国际互联网的攻击的威胁也应继续成为讨论的焦点。信息技术的弱点以及人们对它的日益依赖[447]，使得我们必须将针对关键基础设施的、基于国际互联网的攻击纳入到防止和对抗网络恐怖主义的战略中来。

但是，尽管人们开展了密集的研究，与网络恐怖主义的斗争依然很艰难。对各国不同方法的比较表明，它们的战略中存在许多相似处。[448] 其中一个原因是国际社会认识到了为了应对国际恐怖主义的威胁，需要全球各国携手制定解决方案。[449] 但当前仍无法肯定这种方法是否成功，或者不同的法律体系以及不同的文化背景是否需要采用不同的解决方案。对这一问题的评估带来了一些独特的挑战，原因是除了对重大事件的报告，几乎没有多少可用的数据可用来进行科学分析。在确定恐怖组织使用信息技术时的威胁等级方面，也出现了同样的困难。这些信息大多数时候是保密的，通常只有情报部门才可以使用。[450] 甚至大家对“恐怖主义”这一术语的含义也没有达成一致。[451] 例如，提交美国国会的一份 CRS 报告声明，如果一个恐怖分子通过国际互联网订购了一张前往美国的机票，那么可以证明该恐怖分子在准备其攻击时使用了国际互联网。[452] 这看起来像是一个模糊的论点，原因是不能仅仅因为是恐怖分子订购了机票而将订购机票视为一种与恐怖分子有关的行为。

宣传活动

1998 年，在 30 个外国恐怖组织中，只有 12 个被美国国务院列入黑名单，这些组织在网站上向公众宣传他们从事的活动。[453] 2004 年，美国和平研究所报告，几乎所有的恐怖组织都建立了网站，包括哈马斯、真主党、库尔德工人党和基地组织。[454] 恐怖分子还开始使用视频社区（如 YouTube）来分发视频消息和进行宣传活动。[455] 网站和其他论坛的使用是颠覆破坏分子团体更加注重专业公关

[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.

的标志。[456] 网站和其他媒体用于宣传活动，[457] 描述和公布恐怖组织活动的理由，[458] 并用于招募新成员 [459] 以及联络现有的成员和捐赠者。[460] 最近，网站还用于散发有关处决的视频。[461]

信息收集

国际互联网上可以接触到大量关于可能的目标的信息。[462] 例如，参与建造公共建筑的建筑师，通常会在其网站上发布建筑规划（参见图 21）。如今，各种国际互联网服务都免费提供高分辨率的卫星照片，而在几年前，这些照片只能供世界上极少数的军事机构使用。[463] 此外，还可找到如何制造炸弹的指南，甚至一些虚假训练营，它们以一种远程学习的方式来提供有关如何使用武器的指导。[464] 此外，从搜索机器人那里还可以获得一些没有采取足够保护措施的敏感信息或者机密信息，[465] 并可通过搜索引擎进行访问。2003 年，美国国防部被告知，一本与基地组织有关的训练手册中包含有一些公开发表的、可以用于寻找潜在目标的详细信息。[466] 2006 年，《纽约时报》报道说，在德国一个网站上，居然公布了如何制造核武器的基本信息，它们提供了关于伊拉克制造核武器方法的证据。[467] 澳大利亚媒体也报道了一则类似的事件：关于恐怖分子可能攻击的目标的详细信息被公布在一个政府网站上。[468] 2005 年，德国的新闻媒体报道说，调查人员在两名试图使用自制炸弹攻击公共交通系统的嫌疑人的计算机中，发现了从国际互联网上下载的、关于如何制造爆炸物的指南。[469]

准备在现实世界实施攻击

恐怖分子在准备攻击的过程中可以采用不同的方法来利用信息技术。发送电子邮件或者在论坛上留下消息就是一些例子，这将结合有关通信的内容来讨论。[470] 目前只讨论更为直接的在线准备方法。一些已发表的报告指出，恐怖分子目前在攻击的准备过程中使用了在线游戏。[471] 而国际互联网上存在着各种各样模拟现实世界的在线游戏。此类游戏的使用者可以利用游戏中的角色（化身），

---

[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.
[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,

在虚假世界中采取攻击行动。从理论上讲，这些在线游戏可以用来模拟攻击，但目前尚不确定，在线游戏究竟已在多大程度上牵涉到这种攻击行动中来。[472]

发布训练材料

国际互联网可用于散发培训材料，例如关于如何制造武器以及如何挑选攻击目标的指南。此类材料在网上大量存在。[473] 2008 年，西方的秘密特工发现了一个国际互联网服务器，它为培训材料的交换以及通信提供了基础。[474] 有报告指出，恐怖组织运营不同的网站来协调各种恐怖活动。[475]

通信

恐怖组织对信息技术的使用不限于运营网站和在数据库中开展研究。在 9·11 袭击之后开展的调查中报告，恐怖分子在协调其攻击时使用了电子邮件进行联络。[476] 新闻媒体曾就恐怖组织通过电子邮件互相交换关于目标和攻击者数量的详细指令进行过报道。[477] 通过使用加密技术和匿名通信方式，通信各方可以进一步增加执法机构识别和监控恐怖分子联络的难度。

恐怖分子筹集资金

大多数恐怖组织依赖从第三方获得的资金。追查这些金融交易已经成为 9·11 袭击之后与恐怖主义作斗争的一种重要手段。但这方面的主要困难之一在于以下事实，即发动攻击所需的资金并不一定很多。[478] 在恐怖分子筹集资金时，可以采用几种方式来使用国际互联网服务。恐怖组织可以利用电子支付系统来接受在线捐赠。[479] 他们可以使用网络来公布关于如何捐赠的信息，例如，应当使用哪个银行账号来捐赠。这方面的一个例子是解放党曾经为可能的捐赠者公布过银行账号信息。[480] 另一种方法是进行在线信用卡捐赠。爱尔兰共和军（IRA）就是最先通过信用卡提供捐赠的恐怖组织之一。[481] 对恐怖组织而言，这两种方法都存在一定的风险，即公布的信息会被执法机构发现，并用来追查这些金融交易。因此，这有可能使匿名的电子支付系统变得更加流行。为了不被发现，恐怖组织试图通过一些非可疑的团体，如慈善组织，来掩盖其筹资活动。另一种（与国际互联网有关的）方法是经营虚假的互联网商店。在国际互联网上创建一个在线商店相对比较简单。网络的最大优势之一是业务可以在全世界范围内进行。要证明在这些网站上进行的金融交易不是普通买卖而是为恐

---

[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.
[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.

怖组织提供的捐赠，是非常困难的。这可能需要对每一笔交易进行调查，但如果在线商店是在不同的管辖地经营的，或者使用了匿名的支付系统，那么这样做的难度将非常大。[482]

对关键基础设施实施攻击

除了欺诈和身份盗用等普通的网络犯罪之外，针对关键基础设施的进攻可能成为恐怖分子的新目标。对信息技术的依赖愈来愈高，使关键基础设施变得更易遭到攻击。[483] 针对用计算机和通信网络连接在一起的互连系统而进行的攻击更是这样。[484] 在这些情形中，因对网络实施攻击而造成网络中断，其损失远超单个系统的失效。即使是短时间的服务中断，也可能对电子商务企业造成巨大的经济损失，而且不仅仅对民用设施是这样，对军用基础设施和服务也一样。[485] 调查或者甚至防止这些攻击的发生，是一项独特的挑战。[486] 与物理攻击不同，攻击者不需要出现在攻击现场，[487] 并且在实施攻击的同时，攻击者可以使用匿名通信手段和加密技术来隐藏其身份。[488] 正如以上所强调的那样，对此类攻击的调查需要采用特殊的程序手段、调查技术以及训练有素的调查人员。[489]

关键基础设施被广泛认为是恐怖分子攻击的一大潜在目标，原因是它对一个国家的可持续发展和稳定无疑是至关重要的。[490] 如果某种基础设施丧失作用或遭到破坏，将对国家的国防或经济安全产生重大影响，那么这种基础设施将被认为是一种关键基础设施。[491] 以下这些尤其重要：电力系统、通信系统、天然气和石油储运系统、银行和金融系统、交通系统、供水系统和应急服务系统。“卡特里娜”飓风对美国基础设施和服务的破坏而导致的内乱程度，突显了社会对这些系统可用性的依赖程度。[492]

关键基础设施容易受到基于网络的攻击的弱点，在一些与航空运输有关的事件中得到了明证。

- 世界大多数机场的登机系统都已使用互连的计算机系统。[493] 2004 年，Sasser 计算机蠕虫病毒[494]感染了全世界数百万台计算机，其中就包括一些大型航空公司的计算机系统，导致一些航班被迫取消。[495]

---

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

- 如今，很大一部分机票是网上订购的。航空公司使用信息技术来进行各种操作。所有的大型航空公司都允许其顾客在线购买机票。与其他电子商务活动一样，这些在线业务可能成为攻击者的目标。用来攻击基于互联网的服务的一种常见方法是拒绝服务攻击（DoS）。[496] 2000 年，在短时间内，美国有线新闻网（CNN）、易趣（eBay）和亚马逊（Amazon）等一些知名公司就遭到了拒绝服务攻击。[497] 结果是，一些服务在数小时甚至几天内无法使用。[498] 航空公司同样也受到过拒绝服务攻击的影响。2001 年，德国汉莎航空公司就成为了一次攻击的目标。[499]
- 对针对关键航空基础设施的、与国际互联网有关的攻击而言，另一个潜在的目标是机场控制系统。计算机控制的飞行控制系统的脆弱性，在 1997 年针对美国 Worcester 机场的黑客攻击中得到了充分的暴露。[500] 在此次黑客攻击中，攻击者使机场塔台的电话服务陷入瘫痪，并关闭了用于管理跑道灯光的控制系统。[501]

2.8.2 网络战争

网络战争是指在使用国际互联网的战争中运用信息通信技术。它与网络恐怖主义有大量的相似之处。[502] 最初对网络战争的讨论着重于用以计算机为媒介的攻击或者基于计算机的攻击取代传统的战争。[503] 基于网络的攻击通常比传统的军事行动成本要低，[504] 而且即使是小国，也能实施这种攻击。

图20

近年来，在武装冲突期间，国际互联网已成为信息与宣传交流的一个重要媒介。常常有这样的争论，在冲突进行过程中的关键阶段，是否可能与/或是否合适停止国际互联网的某些服务。

防止网络攻击是很难的。到目前为止，关于用基于国际互联网的攻击替代武装冲突的报告还很有限。[505] 当前的讨论主要还集中于在冲突期间对关键基础设施的攻击以及对情报的控制（参见图 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.

在考虑民用和军用通信的过程中，信息基础设施是军事冲突的一个重要目标。不过，目前尚不确定，这些攻击是否将通过国际互联网来实施。在爱沙尼亚[506]和美国[507]曾发生过的、针对计算机系统的攻击，就与网络战争有一定的关联。由于无法明确地从攻击追踪到某个国家的官方组织，因此，难以将其定性为网络战争。对基础设施实施实质性的攻击（如通过武器和爆炸物），也难以归类为网络战争。[508]

对信息的控制一直是军事冲突中的一个重要问题，原因是信息可以用来影响公众，也可以用来影响军事人员。在军事冲突期间，对国际互联网上的信息实施控制将成为一种越来越重要的影响手段。

2.8.3 网络洗钱

国际互联网正被用于洗钱。尽管数量更大的、传统的洗钱技术仍有诸多优势，但国际互联网也提供了若干优势。在线金融服务为非常迅速地完成多项涉及全世界的金融交易提供了选择方案。国际互联网有助于克服对现实金融交易的依赖。随着在遏制对现实货币的依赖方面迈出第一步，电子转账取代了传统的现金转移，但是，各国政府采取了更加严格的规定来侦查可疑的电子转账，迫使违法者转而研究一些新的技术。在与洗钱犯罪活动作斗争的过程中，对可疑交易的侦查是基于金融机构在转账方面的义务来进行的。[509]

洗钱通常分为三步：

1．布置；

2．分层；以及

3．综合。

关于大量现金的处置，使用国际互联网或许不具备许多实际的优势。[510] 不过，对违法者而言，在分层（或者说掩饰）阶段，国际互联网特别有用。在这种背景下，当洗钱者利用在线赌场进行分层时，要调查网络洗钱就变得特别困难了（参见图21）。[511]

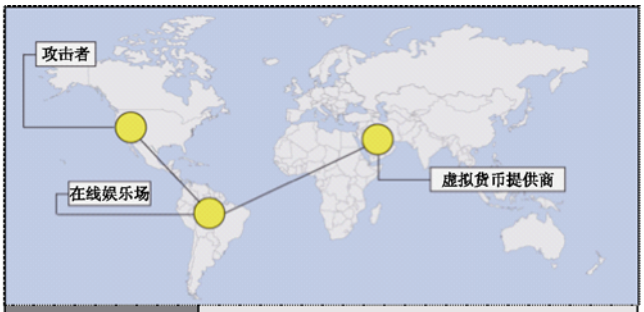


图21

上图说明了在基于国际互联网的洗钱诡计中，在线娱乐场与虚拟货币是如何结合的。利用此类服务，攻击者使执法机构很难跟踪转账过程以及确定攻击者。

[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.

当前，用于管制资金转移的规定很有限，国际互联网为违法者廉价、免税的跨国资金转移提供了可能。目前，在调查基于国际互联网的洗钱技术过程中存在诸多困难，这常常源自虚拟货币和在线赌场的使用。

1. 使用虚拟货币：

推动虚拟货币发展的一个关键因素是小额支付（例如，为了支付网上下载一篇文章不到 10 美分的费用），这种时候，使用信用卡就成了问题。随着小额支付的需求日益增大，包括“虚拟金币”在内的虚拟货币应运而生。虚拟金币是以账号为基础的支付系统，金币的价格靠黄金储备来支持。用户可以在线开设电子金币账号，通常无需注册。有些提供商甚至能够进行直接的点对点（个人对个人）转账或者现金提款。[512] 违法者可以在不同的国家开设电子金币账号，并且将它们结合起来，使为了洗钱和资助恐怖活动而使用金融工具变得更加复杂化。账号持有者还可以在注册期间使用不准确的信息来掩盖其身份。[513]

2. 使用在线赌场：

与开设实际的赌场不同，开设在线赌场无需大笔的金融投资。[514] 此外，各国对在线和离线赌场的管制通常各不相同。[515] 只有当赌场留有详细记录，

并将它们提供给执法机构时，才有可能跟踪资金转移情况，证明所转资金并非赢来的钱，而是洗钱的结果。

当前对基于国际互联网的金融服务的法律管制，不如对传统金融服务的管制那样严格。除了这种法律上的差异之外，管制的困难还来自以下几个方面：

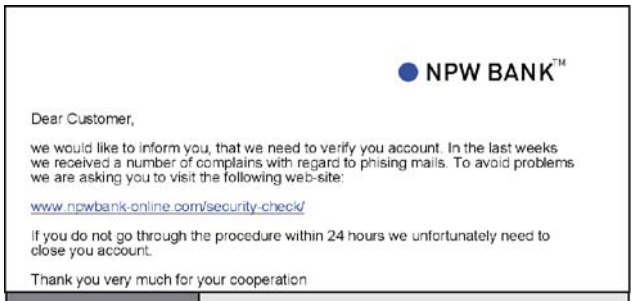
- 难以进行客户验证：如果金融服务提供商和客户从不见面，那么准确的验证可能只是流于形式；[516]
- 由于缺乏个人合同：难以应用传统的“认识你的客户”程序；以及
- 国际互联网转账常常涉及许多国家中提供商的跨国参与；
- 当提供商允许客户以点对点模式转移资金时，由于缺少相应的法律/刑法，使得监控某些手段的工作变得异常困难。

[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.

2.8.4 网络钓鱼

违法者已经开发了一些技术来从用户手中获取个人信息，包括刺探程序[517]和“网络钓鱼”攻击。[518]“网络钓鱼”指的是想方设法使受害者泄露个人/秘密信息的违法行为。[519]有各种不同类型的“网络钓鱼”攻击，[520]但基于电子邮件的网络钓鱼攻击包含三个主要阶段。在第一个阶段中，违法者确定提供在线服务的合法公司，并与它们瞄上的客户进行电子通信，如金融机构。违法者设计一些类似于合法网站的网站（“钓鱼网站”），要求受害者执行通常的登录程序，这样，违法者就可以获得受害者的个人信息（如账号和在线银行密码）。

为了使用户能够进入这些经过伪装的欺骗网站，违法者向他们发送类似于合法公司发出的电子邮件（参见图 22），[521]这往往还导致商标侵权。[522]这种冒充合法公司发出的电子邮件要求接收者登录，以便更新或者进行安全检测，或者，假如用户不肯合作，违法者就采用威胁手段（如威胁关闭用户的账号）。这种冒充的电子邮件往往包含一个链接，将使受害者点击后进入欺骗网站，以避免用户手动输入合法金融机构的正确网址。违法者还研发了一些先进的技术来防止用户意识到他们进入的不是真正的金融机构网站。[523]


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

图22

网络钓鱼电子邮件设计得看起来像是一个来自合法公司的电子邮件，以使受害者透露秘密信息。攻击者的目标常常是金融机构的客户。

[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.
[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.

一旦个人信息被泄露，违法者就会登录受害者的账号，并实施各种犯罪，如转移资金、申请护照或新账号等。“网络钓鱼”成功攻击的数量在增多，证明了它的破坏潜力。[524] 2007 年 4 月[525]，向反网络钓鱼工作组（APWG）[526] 报告的、特别的“网络钓鱼”网站超过了 55000 家。“网络钓鱼”技术不仅限于获取在线银行业务的密码。违法者还试图获取进入计算机的密码、拍卖平台和社会保险号，这些在美国都是特别重要的信息，可以导致“身份盗用”违法行为的发生。[527]

2.9 网络犯罪的经济影响

毋庸置疑，由计算机和国际互联网犯罪造成的经济损失是巨大的。最近公布的各种调查对网络犯罪的经济影响进行了分析，[528] 强调了它对经济的重要影响。对这种犯罪的统计数据，还有另一种同样普遍的担心，就是对经济损失的估计也许不太准确 — 无法确定这些调查到底在多大程度上提供了准确的统计数据和结果，原因是许多受害者并没有报告此类犯罪行为。[529]

2.9.1 所选调查结果概述

美国计算机安全协会（CSI）于 2007 年开展的计算机犯罪与安全调查，对网络犯罪的经济影响进行了分析，[530] 其依据是 494 位在美国公司、政府机构和金融机构中的计算机安全从业者的回复，主要针对的是美国的情况。[531]

考虑到经济周期，调查结果表明，在 2002 年之前，网络犯罪造成的经济损失数额是上升的，但在此之后的第二年，其数额出现了下降。这一调查表明，其结果是有争议的，但尚不清楚为什么报告的网络犯罪数量以及受害者的平均损失会有所下降。2006 年，损失数额再一次上升。调查也没有解释为什么 2002 年报告的损失会减少或者 2006 年会上升。从报告确定的 21 类网络犯罪来分析，造成经济损失最惨重的网络犯罪涉及金融欺诈、病毒、系统渗入以及窃取机密数据。2006 年，所有回复者总的损失金额约高达 6690 万美元。

---

[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/.

每位回复者平均的损失金额在出现了几年的下降后，网络犯罪造成的损失转而上升。2006 年，平均损失为 345000 美元。2001 年，平均损失是这一金额的近 10 倍（310 万美元）。每位回复者平均的损失在很大程度上取决于回复者的组成（如果头一年回复的主要是中小型企业，而第二年回复的是较大型企业，那么参与者组成的变化将严重影响到统计结果）。

美国联邦调查局（FBI）2005 计算机犯罪调查[532] 采用的方法与 CSI 所用的调查方法类似，但其覆盖面更为广泛。[533] 联邦调查局的调查估计，计算机和国际互联网犯罪带来的安全事件造成的损失高达 2170 万美元。[534] 回复组织察觉的最常见的违法行为是病毒攻击、刺探程序、端口扫描以及破坏数据或网络。[535] 联邦调查局 2005 计算机犯罪调查包括对网络犯罪对美国经济总的损失的估计。[536] 基于被调查者报告的平均损失 [537] 以及假设美国 20%左右的组织都受到了网络犯罪的影响，计算得出的总的损失高达 670 亿美元。[538] 不过，还有人担心这些估计值是否具有代表性，并担心每年的参与者是否一致。[539]

2007 年计算机经济学恶意软件报告 [540] 主要关注的是恶意软件对全球经济造成的影响，方法是将攻击造成的估计损失 [541] 累加起来，其中一个重要发现是，设计恶意软件的违法者开始从以破坏为目的转向以牟利为目的。该报告发现，因恶意软件攻击造成的经济损失在 2000 年和 2004 年达到了高峰，分别为 171 亿美元和 175 亿美元，而从 2004 年后，则一直呈下降趋势，到 2006 年降至 133 亿美元。不过，与这一调查结果类似，关于恶意软件对经济影响的数据是否切合实际仍存在一些不确定性。报告的损失与证明的损失之间存在巨大差别 — 以 Sasser 蠕虫病毒为例。有数百万个计算机系统报告被感染。[542] 但在对软件设计者提起的民事诉讼中，几乎没有哪家公司和个人对法庭要求证明其遭受损失并加入诉讼的请求做出了回应。这一案件最终的判决结果是，病毒设计者只需赔偿不到 1 万美元的损失。[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 网络犯罪统计相关的困难

尚不清楚有关网络犯罪对经济影响的这些统计数据是否具有代表性，以及它们是否提供了关于损失程度的可靠信息。[544] 也不明确对网络犯罪的报告究竟到了何种程度，不仅指在调查中的报告，还指对执法机构的报告。从事与网络犯罪作斗争的主管部门鼓励受害者报告这些犯罪。[545] 使用关于网络犯罪真实事件的更为准确的信息，将使执法机构能够更加有力地起诉违法者，阻止潜在的攻击，并制定更恰当、更有效的法律。

有些公共和私营部门试图量化恶意软件造成的直接和间接损失。要估计它对企业造成的损失已经很难，要评估恶意软件对企业以及可能对个人消费者造成的经济损失会更难，尽管不时有证据表明损失相当巨大。[546] 不过，此类损失的构成是不同的。恶意软件可以造成对硬件和软件的直接破坏，以及因身份盗用或其他欺诈案件而造成的经济损失和其他损失。尽管不断出现的总的情况都差不多，但估值范围会有所不同。

另一方面，出于若干理由，企业也许会不报告网络犯罪行为：

企业害怕这种负面新闻破坏其声誉。[547] 如果一家公司宣布黑客访问了其服务器，也许会失去用户的信任。这导致的全部成本和后果，可能大于黑客攻击带来的损失。不过，如果攻击者不被报告，不遭到起诉，那么他们可能继续作案。

受害者也许不相信执法机构能够找到攻击者。[548] 比较大量的网络犯罪案件与极少数的成功调查，受害者会认为报告网络攻击行为几乎没有多少价值。[549]

自动化也意味着网络犯罪作案者可以采用以下策略，即通过发动大量攻击来牟取巨大利益，但对每个攻击对象只造成少量的损失（例如，预付费欺诈采用的就是这种策略[550]）。对小额损失，受害者也许宁愿不去费时地报案。往往只有在遭受巨大损失时才报案。[551] 使攻击对象只遭受少量损失，这样，攻击者设计的骗局常常不会被执法机构跟踪调查。

---

[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. 与网络犯罪作斗争面临的挑战

信息通信技术的最新发展不仅产生了新的网络犯罪方法和新的犯罪方法，也为调查网络犯罪带来了新的方法。信息通信技术的进步极大增强了执法机构的能力。与之相对的是，违法者也可使用新的工具来防止被识别，并阻碍执法机构对案件的调查。本章着重阐述与网络犯罪作斗争所面临的挑战。

3.1 机会

如今，执法机构可以使用功能日益强大的计算机系统和复杂的取证软件来加速调查和自动执行搜索程序。[552]

自动调查过程证明是困难的。虽然根据关键字搜索非法内容可以很容易地进行，但要识别非法图片则存在更大的问题。只有当图片此前已被定级，散列值已保存在数据库中，而且所分析的图片没有进行过修改，才能成功运用基于散列值的方法。[553]

通过将嫌疑人硬盘上的文件与已知图片的信息进行比较，取证软件能够自动搜索儿童色情图片。例如，2007 年年底，主管部门发现了大量的儿童性虐待照片。违法者为了防止其身份被识别，在把图片发布在国际互联网上之前，对其脸部部分图片用数字方法进行了修改（参见图 23）。计算机取证专家可以拆解所做的修改，并重构嫌疑人的脸部图像。[554] 尽管成功的调查清楚地展示了计算机取证的潜力，但这一案例并不能就证明在儿童色情案件调查方面取得了突破。如果犯罪嫌疑人只是简单地用白点盖住其脸部图像，那么将无法识别其身份。

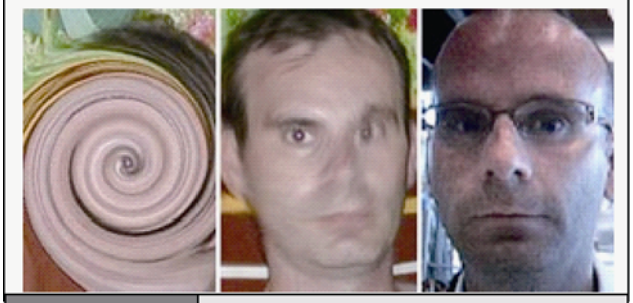


图23

在上例中，计算机取证专家能够除去对照片所做的修改，并重构嫌疑犯的脸部。

[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 一般挑战

3.2.1 对信息通信技术的依赖

许多日常通信依赖信息通信技术和基于国际互联网的服务，包括 VoIP 电话或电子邮件通信。[555] 当前的信息通信技术承担着控制和管理建筑物、[556] 汽车和航空业务的作用（参见图 24）。[557] 供能、供水以及通信服务都要依赖信息通信技术。信息通信技术有望进一步融入人们的日常生活。[558]

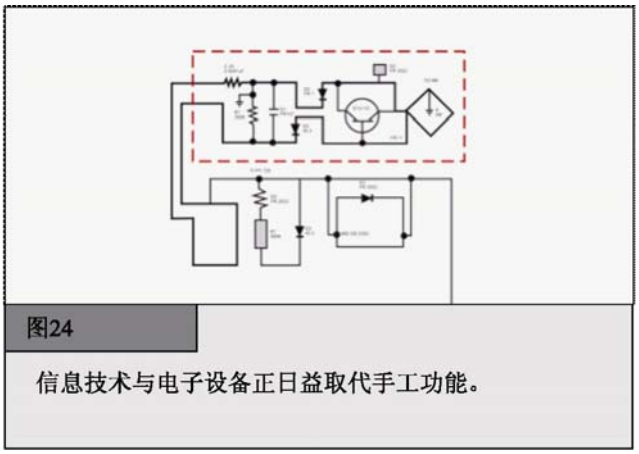


图24

信息技术与电子设备正日益取代手工功能。

对信息通信技术的日益依赖使得系统与服务越来越容易受到针对关键基础设施的攻击的威胁。[559] 即使是短时间的服务中断，也可能造成电子商务企业的巨额损失[560] — 攻击不仅会使民用通信中断；对信息通信技术的依赖对军用通信而言也是一个巨大的威胁。[561]

现有的技术基础设施存在许多弱点，如操作系统的单一性或者同质性。许多个人用户和中小型企业（SME）使用微软公司的操作系统，[562] 因此，攻击者可以专门针对这一种目标来涉及有效的攻击方法。[563]

---

[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.

社会对信息通信技术的依赖，不仅仅限于西方国家，[564] 发展中国家同样也在防止基础设施和用户遭受网络攻击方面面临挑战。[565] 更廉价基础设施技术的发展，如 WiMAX，[566] 使发展中国家能为本国更多的人民提供国际互联网服务。发展中国家可以避免有些西方国家曾经犯过的错误，这些国家过于关注如何尽可能实现网络和服务的可达性，而没有在安全保护措施方面进行大的投资。美国的专家解释说，发生在爱沙尼亚的、对政府组织官方网站的成功攻击，[567] 可能仅仅是由于未采取足够的保护措施而引起的。[568] 发展中国家拥有独特的机会来较早地整合安全措施。这也许需要更大的前期投入，但从长远来看，整合安全措施的时间越晚，所需付出的代价将越大。[569]

必须制定出有效的战略来防止此类攻击，并提出应对攻击的对策，包括发展和推广技术保护手段，以及制定能够有效打击网络犯罪的、适当而充分的法律。[570]

3.2.2 用户数量

国际互联网及其服务受欢迎的程度与日俱增，目前全世界有 10 多亿国际互联网用户（参见图 25）。[571] 计算机公司和国际互联网服务提供商正将目光聚集到发展中国家，因为这些国家拥有最大的、进一步发展的潜力。[572] 2005 年，发展中国家的国际互联网用户数量第一次超过了工业化国家，[573] 与此同时，廉价硬件以及无线接入的发展将可使更多的人们接入国际互联网。[574]

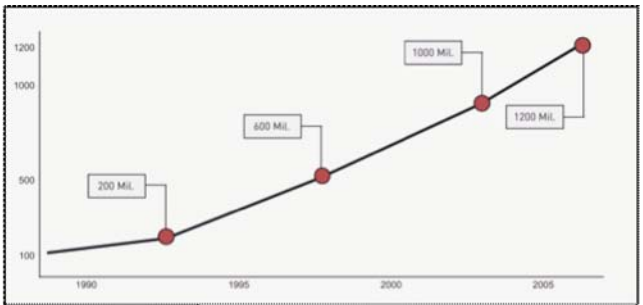


图25

目前有10亿多国际互联网用户。

[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.
[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.

随着接入国际互联网的人数愈来愈多，攻击者及其攻击目标的数量也将增多。[575] 难以估计有多少用户在利用国际互联网从事非法活动。即使只有 0.1%的用户利用国际互联网来从事违法活动，那么违法者的总数也将超过 100 万。尽管发展中国家的国际互联网使用率较低，但推动网络安全却并不容易，原因是违法者可以从世界任何角落来实施违法行为。[576]

国际互联网用户数量的增多也给执法机构带来了难题，原因是要自动执行调查过程相对较难。虽然采用基于关键字的方法来搜索非法内容可能十分容易，但要识别非法图片是一个更大的问题。例如，只有当图片此前被定级，散列值已保存在数据库中，而且所分析的图片没有进行过修改，才能成功运用基于散列值的方法。[577]

3.2.3 设备与访问的可用性

实施计算机犯罪只需要一些基本的设备，通常包括：

- 硬件；
- 软件；以及
- 国际互联网接入。

谈到硬件，计算机的威力仍在继续增强。[578] 为使发展中国家更广泛地使用信息通信技术，各国提出了一系列倡议。[579] 罪犯只需要使用廉价的或者二手的计算机技术就可以实施严重的网络犯罪，在这里，知识远比设备有价值得多。可用的计算机技术是新是旧，对使用这种设备来实施网络犯罪而言几乎没有任何影响。

借助专业的软件工具，可以更容易地实施网络犯罪。攻击者可以下载一些专用于定位开放端口或者破解密码保护 [580] 的软件工具。[581] 由于镜像技术和点对点交换技术的存在，限制此类工具的推广应用是困难的。[582]

---

[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.

[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] *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.

[581] "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.

[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.

最后一个必不可少的要素是国际互联网接入。尽管大多数发展中国家的国际互联网接入费用[583]高于工业化国家，但发展中国家的国际互联网用户数量正在急剧增加。[584]攻击者一般不会预订一种国际互联网服务，以减少被识别的概率，他们更喜欢无需（经过验证的）注册就可以使用的服务。接入网络的一种典型方法是所谓的“四处逛荡”。这一术语用于描述四处逛荡以寻找可接入无线网络的行为。[585]攻击者最常用的网络连接方法是：

- 公共国际互联网终端；
- 开放（无线）网络（参见图 26）；[586]
- 被黑的网络；以及
- 无需注册的预付款服务。

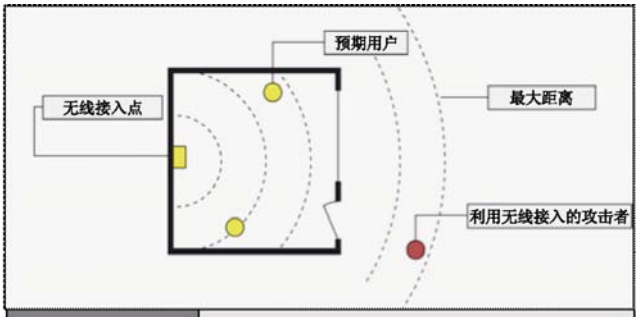


图26

接入国际互联网而不留下踪迹是许多攻击者的优先选择。图形显示了一个攻击者如何使用开放无线网络的信号来实现远程接入。在这些情况下，几乎无法确定攻击者。

执法机构正在采取措施，限制这种不受控制的国际互联网服务接入，以避免罪犯滥用这些服务。例如，在意大利和中国，使用公共国际互联网终端要求提供使用者的身份。[587]不过，对于这种身份要求，存在一些争议。[588]尽管对接入的限制可以防止犯罪并方便执法机构的调查，但此类规定可能阻碍信息社会和电子商务的发展。[589]有人认为，对国际互联网接入的这种限制有可能侵犯人权。[590]例如，欧洲法庭在许多有关广泛的案件中裁定，自由表达的权利不仅仅适用于信息的内容，也适用于发射或接收的方法。在瑞士 Autronicv.公司的案件中[591]，法庭坚称，由于任何强加于接入方法上的限制都将干扰接收和传送信息的权利，因此有必要作出进一步的解释。如果这些原则应用于对国际互联网接入的潜在限制，那么此类法律措施可能造成对人权的侵犯。

[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
[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.

3.2.4 信息的可用性

国际互联网上拥有数百万个网页，[592] 上面都是一些最新的信息。任何一个公布或维护一个网页的人都可以参与。维基百科（Wikipedia）就是由用户自己产生的平台的一个成功例子，[593] 它是一部任何人都可以发布信息的在线百科全书。[594]

国际互联网的成功还取决于强大的搜索引擎，它们可以使用户在数秒钟内搜索到数百万个网页。这一技术既可用于法律目的，也可用于实施犯罪。“谷歌黑客”或者“谷歌剁客”指的是使用复杂的搜索引擎查询来过滤大量的搜索结果，以寻找与计算机安全问题相关的信息。例如，攻击者可能着眼于搜索不安全的密码保护系统。[595] 报告强调了非法使用搜索引擎的风险。[596] 打算进行攻击的攻击者，可以在国际互联网上找到关于如何使用能够在普通超市中买到的化学物质来制造炸弹的详细信息（图 27）。[597] 尽管此类信息即使在国际互联网问世之前同样也可以获得，但不管怎样，以前要获得此类信息要困难得多。如今，任何国际互联网用户都可以接触到此类指南。

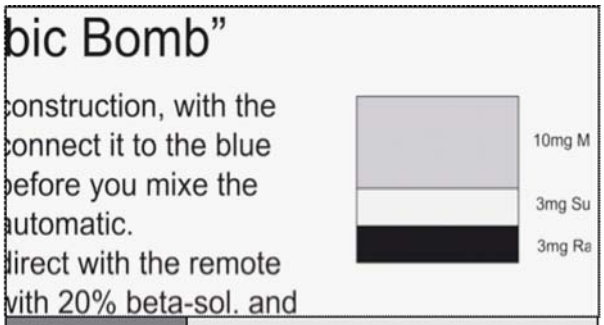


图27

在国际互联网的许多网站上都可以找到如何制造武器和炸药的说明书。图形显示的是如何仅使用从药店就可获得的部件来制造一枚炸弹的说明。

罪犯还可以使用搜索引擎来分析攻击目标。[598] 在调查恐怖组织成员的过程中，调查人员发现了一份培训手册，这突显了国际互联网在收集可能的目标方面能够发挥巨大的作用。[599] 使用搜索引擎，攻击者能够收集到公开的有用信息（如公共建筑物的建筑规划），这将有助于其准备攻击行动。有报道指出，攻击在阿富汗的英军部队的武装分子就使用了来自谷歌地球（Google Earth）的卫星图片。[600]

---

[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.

[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.

3.2.5 失去控制机制

所有的大规模通信网络，从用于语音电话的电话网络到国际互联网，都需要中央控制和技术标准，以确保操作性。当前关于国际互联网管理问题的讨论表明，与国家甚至跨国通信基础设施相比，国际互联网并没有什么不同。[601] 国际互联网也需要受到法律的制约，立法者和执法机构已经开始制定一些法律标准，以便对国际互联网实施一定程度的中央控制。

国际互联网最初是设计为一种军事网络，[602] 它基于一种分散的网络体系结构，旨在保持主要功能的完整和有效，即使在网络的组成部分受到了攻击时。结果是，国际互联网的网络基础设施对外部的控制意图具有抵抗性。最初的设计并非为了便于犯罪调查或者防止来自网络内部的攻击。

如今，国际互联网在民用服务中的使用越来越广泛。随着从军用转向民用，对控制手段的需求特性也发生了变化。由于网络基于为军事用途而设计的协议，因此并不存在这些中央控制手段，而且如果不对网络进行重大的重新设计，是难以追溯式地来实施控制的。缺少控制手段使得对网络犯罪的调查变得十分困难。[603]

由于缺乏控制手段而引发问题的一个例子是使用加密匿名通信服务[604] 的用户可以绕过过滤技术。[605] 如果接入提供商拦阻含有非法内容（如儿童色情）的某些网站，用户一般将无法访问它们。但是，如果用户在他们与中央服务器之间使用匿名通信服务器加密通信，那么就可以避开对非法内容的拦阻。在这种情况下，提供商可能无法拦阻这些请求，原因是对作为加密消息发送的请求，访问提供者也无法打开（图 28）。

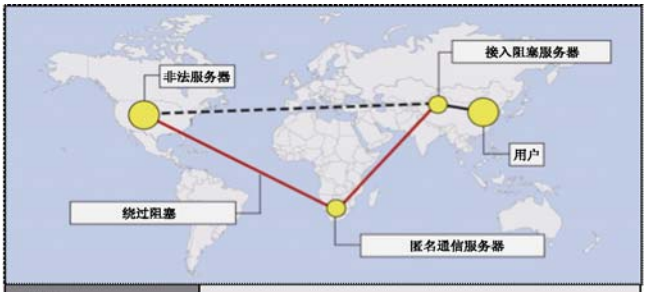


图28

图形显示了绕过接入提供商安装的中央控制机制的可能性。如果接入提供商安装了某种过滤技术，那么用户请求将被阻塞。如果用户利用匿名通信服务器对请求进行加密，那么可绕过这种控制方法。例如，在这种情况下，接入提供商不触及发往匿名通信服务器的请求，因此无法阻塞该网站。

[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.
[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 3.2.12.

3.2.6 国际影响

许多数据传送过程会影响到多个国家。[606] 如果直接链路被临时阻断，那么用于国际互联网数据传送的协议将基于最理想的路径。[607] 甚至在发起国中的国内传送过程受到限制时，数据也可以离开这个国家，并传送到境外的路由器上，并重新导回到其最终目的地所在的国家。[608] 此外，许多国际互联网服务基于国外的服务，[609] 例如，托管服务提供商可以基于一个国家的硬件来在另一个国家提供网络空间租用服务。[610]

如果攻击者和攻击对象位于不同的国家，那么网络犯罪调查需要所有受影响国家的执法机构的合作。[611] 国家主权不允许未经当地主管部门的同意就在别国的领土范围内开展调查。[612] 网络犯罪调查需要所有相关国家主管部门的支持与参与。

在应对网络犯罪时，难以根据传统的相互法律援助原则来开展合作。与国外执法机构协调所需的正式要求以及所需的时间，常常阻碍网络犯罪调查的开展。[613] 调查常常要在非常短的时间周期内进行。[614] 跟踪违法行为所需的关键数据常常会在很短的时间后便会被删去。这样短的调查时间是有问题的，原因是传统的相互法律援助体系常常需要花时间来组织。[615] 如果调查中的违法行为在某个相关国家不被认为是有罪的 [616]，那么双重犯罪原则 [617] 也会带来一些难题。攻击者可能故意在其攻击中纳入第三国，以增加网络犯罪调查的难度。[618]

---

[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.

[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.

罪犯可能故意选择本国之外的目标，并且从那些对网络犯罪立法不够严格的国家开始行动（图 29）。[619] 与网络犯罪有关的法律协调以及国际合作，将有助于应对这些问题。在网络犯罪调查中促进国际合作有两种方法：一是八国集团的 24/7 网络；[620] 二是欧洲理事会《网络犯罪公约》中与国际合作有关的规定。[621]

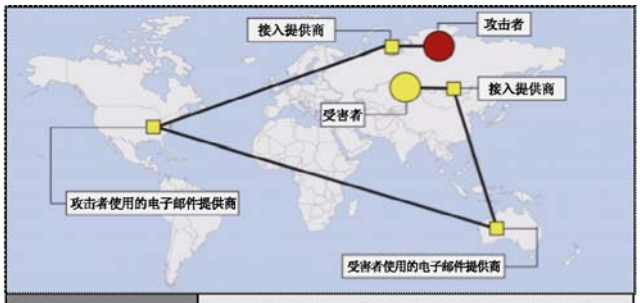


图29

图形显示，即使攻击者与目标处于同一个国家中，也可实施发送带有非法内容电子邮件的行动，并跨越不同的国家。即使不是这样，在重新传回之前，数据传送过程也可在某个国家之外进行。

3.2.7 现场外的远程犯罪

罪犯不必出现在目标对象所在的同一地点。由于罪犯的位置可与犯罪现场完全不同，因此许多网络违法行为是跨国的。国际性的网络犯罪行为要耗费大量的精力和时间。网络罪犯力求避开那些具有严格网络犯罪立法的国家（图 30）。[622]

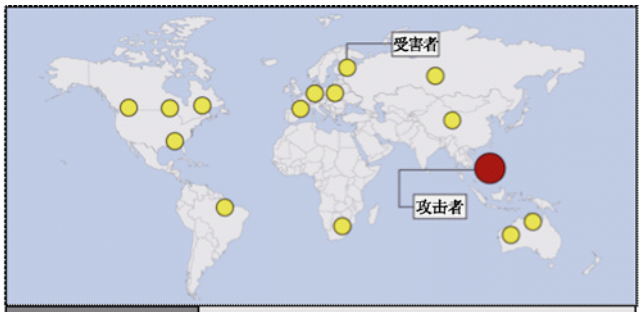


图30

攻击者几乎可以在世界任何地方接入国际互联网来实施攻击。潜在攻击者在决定从何处发起攻击时需考虑的主要问题包括：网络犯罪立法状况、执法机构的效能以及匿名国际互联网接入的可用性。

在与网络犯罪作斗争的过程中，防止“安全避风港”的出现是其中的一项关键挑战。[623] 一旦存在“安全避风港”，违法者将利用它们来阻止犯罪调查。尚未实施网络犯罪法律的发展中国家可能变得容易受到攻击，原因是罪犯可选择以这些国家作为基地，以避免遭到起诉。由于违法者处在法律不健全的国家中，因此难以阻止会影响到全球受害者的严重违法行为。这可给某些特定的国家施加一定的压力，迫使它们考虑通过法律来制裁网络犯罪。这方面的一个例子是：2000 年，一位犯罪嫌疑人在菲律宾开发出了“爱虫”计算机蠕虫病毒，[624] 该病毒感染了全世界数百万台计算机。[625] 但由于当时

[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.
[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.

的菲律宾尚未对研发和传播恶意软件的行为做适当的定罪，因而使得当地的调查工作受阻。[626] 另一个例子是尼日利亚，它曾受到国际压力，被迫针对借助电子邮件进行的金融骗局采取行动。

3.2.8 自动化

信息通信技术的最大优势之一是能够自动执行某些过程。自动化的若干主要优势是：

- 它加速了过程的进展；
- 它扩大了过程的范围，增强了其影响；
- 它限制了人类的参与。

自动化减少了对成本密集的人力的需求，使提供商能够以更低的价格来提供服务。[627] 攻击者可以利用自动化来扩大其犯罪活动的规模 — 数百万条主动发出的垃圾邮件 [628] 短信可以借助自动化方式发出[629]（参见图 31）。如今，黑客攻击常常也是自动进行的，[630] 每天有多达 8000 万次的黑客攻击 [631] 是因使用软件工具而自动进行的，[632] 它们可以在数小时内对数千个计算机系统实施攻击。[633] 借助自动化过程，攻击者可以通过设计骗局来牟取暴利，这些骗局基于数量巨大的攻击，每个受害者蒙受的损失相对较小。[634] 单个受害者的损失越小，受害者就越有可能不会报告自己所遭受的攻击。

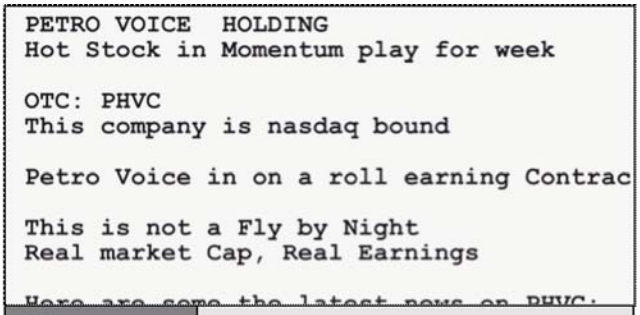


图31

自动处理的一个例子是垃圾邮件的分发。在一个很短的时间内就可以发出几百万封电子邮件。

攻击自动化对发展中国家的影响尤其显著。由于它们的资源有限，因此相比工业化国家，发展中国家因垃圾邮件而造成的问题将更加严重。[635] 通过自动化来实施的犯罪数量越大，对全世界执法机构的挑战就越严峻，原因是在其管辖范围内不得不需要准备面对更多的受害者。

---

[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.

[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

3.2.9 资源

目前进入市场的现代计算机系统的功能非常强大，可以用于扩大犯罪活动的规模。但并不是仅仅因单个用户计算机性能的增强而给调查带来了诸多问题，[636] 网络容量的增大也是一个主要问题。

最近的一个攻击案例是对爱沙尼亚政府网站的攻击。[637] 对这些攻击的分析表明，它们是通过一个“僵尸网络”[638] 上的成千上万台计算机来实施的，或者是在外部控制下运行程序的一组受到危害的计算机来实施的。[639] 在大多数情况下，受到恶意软件感染的计算机都安装了一些工具，使作案者可以对其实施控制（参见图 32）。僵尸网络用于收集与目标有关的信息，或者实施高水平的攻击。[640]

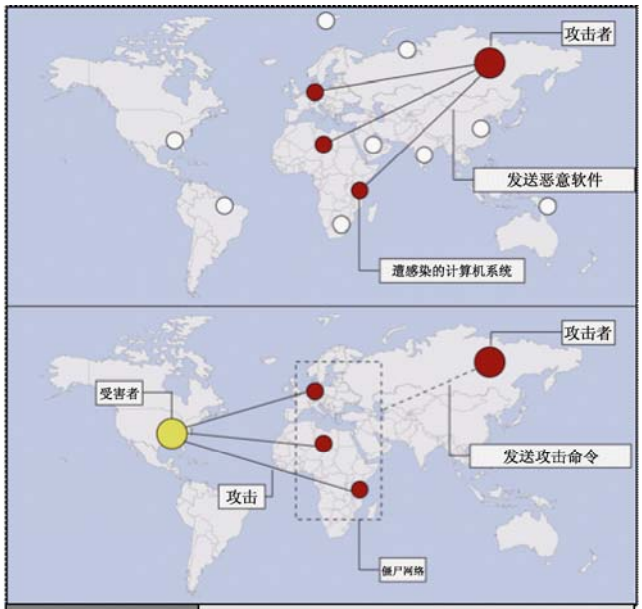


图32

以上两个图显示了制造和使用一枚炸弹的过程。

最近几年，僵尸网络已成为网络安全的一个严重威胁。[641] 僵尸网络的规模可大可小，小到几台计算机，大到 100 多万台计算机。[642] 当前的分析表明，在连接到国际互联网的所有计算机中，有多达四分之一的计算机可能被恶意软件感染，使之成为僵尸网络的一部分。[643] 僵尸网络可以用于各种犯罪活动，包括：

- 拒绝服务攻击；[644]
- 发送垃圾邮件；[645]
- 黑客攻击；以及
- 文件共享网络。

---

[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;
[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.

僵尸网络为攻击者提供了诸多优势。它们增强了罪犯的计算机与网络能力。使用成千上万个计算机系统，罪犯可以攻击其他遥不可及的计算机系统，只需少量的计算机来引导攻击行动。[646] 僵尸网络还使执法机构更难跟踪最初的攻击者，原因是最初的跟踪线索只导向僵尸网络的成员。由于罪犯控制着更为强大的计算机系统与网络，因此调查部门的计算机系统与网络的能力与那些处在罪犯控制之下的计算机系统与网络的能力之间的差距正变得越来越大。

3.2.10 数据交换处理的速度

在国与国之间传送电子邮件只需几秒钟的时间。这么短的时间也是国际互联网取得成功的理由之一，电子邮件大大缩短了物理传送消息的时间。不过，如此迅速的数据交换也给执法机构带来了困难，因为几乎没有给它们留下多少调查或收集证据的时间。传统的调查通常需要花费更长的时间。[647]

这方面的一个例子是儿童色情内容的交换。过去，色情视频是亲手交给购买者或者发货给购买者。这两种方法都给执法机构进行调查提供了机会。儿童色情内容的国际互联网在线与离线交易之间的主要差别在于传输。如果违法者使用国际互联网，那么视频内容的交换可以在数秒钟内完成。

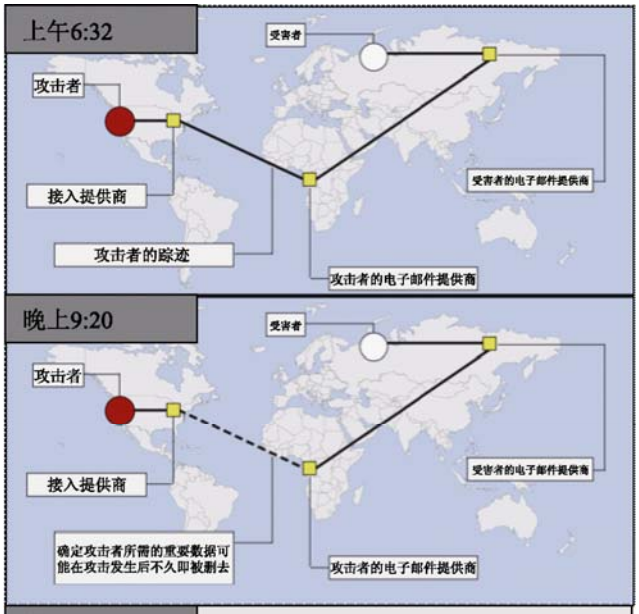


图33

图形显示了在网络犯罪调查中即时作出响应的重要性。在发送电子邮件过程中产生的重要数据以及可用于确定攻击者的重要数据，常常在电子邮件发送后不久即被删去。没有这些数据，确定攻击者往往是不可能的。

电子邮件还展示了可以立即付诸使用的即时反应工具的重要性（参见图 33）。为了跟踪和识别犯罪嫌疑人，调查人员通常需要访问一些数据，而这些数据在传输之后可能很快就被删去。[648] 调查机构要求在很短的时间内作出反应，这对于成功的调查至关重要。没有使调查人员能够迅速作出反应且阻止数据被删除的恰当的法律和工具，是无法有效地与网络犯罪作斗争的。[649]

“快速冻结程序”[650] 以及 24/7 网络点[651] 是可以提高调查效率的工具的例子。针对数据保留的立法还着眼于增加执法机构进行调查时可用的时间裕量。如果在一段时间内保留了跟踪违法者所需的数据，那么执法机构成功识别犯罪嫌疑人的机率就会更大。

---

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.
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.

3.2.11 发展速度

国际互联网不断在发展。图形用户接口（WWW [652]）的问世标志着它开始迅速扩展，原因是过去一些基于命令的服务不够用户友好。WWW 的问世还使一些新的应用以及新的犯罪活动 [653] 成为可能 — 在这方面，执法机构正在努力追赶。进一步的发展仍在继续，主要表现在：

- 在线游戏；以及
- 网际协议语音服务（VoIP）通信。

在线游戏更为流行，但目前尚不清楚执法机构是否能够成功调查和起诉在这一虚拟世界中实施的违法犯罪活动。[654]

从传统的语音电话到国际互联网电话的转变，也对执法机构提出了新的挑战。由执法机构开发的、用于截获传统手机通信的方法和程序，通常无法用于 VoIP 通信。对传统语音电话的截获通常要通过电信提供商来进行。将相同的原则运用于 VoIP，执法机构将需要通过 ISP 以及提供 VoIP 服务的服务提供商来进行。不过，如果服务基于点对点技术，那么服务提供商一般无法截获通信，原因是相关的数据是在通信各方之间直接传输的。[655] 因此，需要一些新的技术。[656]

采用新的网络技术的硬件设备也正在迅速发展中。最新的家庭娱乐系统将电视转变成了国际互联网接入点，而最新的移动式手持设备可以存储数据，并且能够通过无线网络连接到国际互联网。[657] 容量超过 1 GB 的 USB（通用串行总线）存储设备已经集成到手表、钢笔和小刀中。执法机构需要在其工作中考虑到这些发展 — 不断对网络犯罪调查人员进行培训，使他们能够及时掌握最新技术，并能够识别相关的硬件以及任何需要掌握的特殊设备，这是一项至关重要的工作。

另一个挑战是无线接入点的使用。无线国际互联网接入在发展中国家的扩张是一个机会，对执法机构而言，则是一个挑战。[658] 如果违法者使用不需要注册的无线接入点，那么执法机构将更难跟踪违法者，原因是调查只能引向接入点。

---

[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.
[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.

3.2.12 匿名通信

某些国际互联网服务的发展使执法机构难以识别违法者。[659] 匿名通信的可能性或者只是某种服务的附带服务，或者是出于避免用户劣势的考虑而提供的。此类服务的例子（甚至可以将它们结合起来）（参见图 34 和图 35）包括：

- 公共国际互联网终端（例如，在机场的终端或网吧）；[660]
- 无线网络；[661]
- 无需注册的预付费移动服务；
- 无需注册的、为主页提供的存储容量；
- 匿名通信服务器；[662]
- 匿名信件转发器。[663]

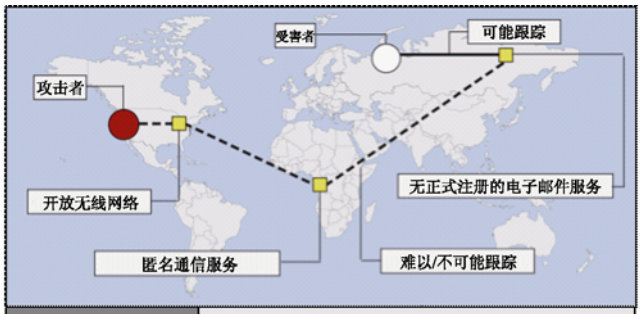


图34

图形说明了攻击者如何通过不同方法的结合来实现匿名。开放无线网络的使用几乎使得无法确定攻击者。利用无需验证注册信息的匿名通信服务和电子邮件服务，攻击者可减少被成功识别的机会。

例如，违法者可以通过使用伪造的电子邮件地址来隐藏其身份。[664] 许多提供商提供免费的电子邮件地址。即使是应当输入个人信息的地方，也可能不需要进行验证，因此，用户可以在不泄露其身份的情况下注册电子邮件地址。例如，如果用户希望加入政治话题讨论团体而不泄露其身份，那么匿名的电子邮件地址就是有用的。匿名通信可能导致反社会行为，但它们也使用户能够更加自由地开展活动。[665]

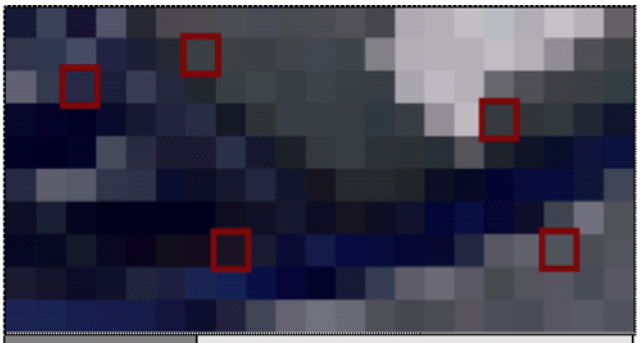


图35

图形说明了如何将信息隐藏在一张图片中。通过修改某些像素的颜色信息，加密软件纳入信息。如果图片足够大，那么不访问原始图片将几乎无法识别所做的修改以及修改后的图片。利用该技术，攻击者可隐藏其正在交换额外信息的事实。

考虑到用户留下的各种线索，显示了需要利用一些手段来防止用户描绘特征剖面的行为。[666] 因此，世界各国和组织都支持匿名使用国际互联网电子邮件服务的原则，例如，在《欧盟关于隐私与电子通信的指令》中就明确

[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;
[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.

表达了这一原则。[667] 用法律手段来保护用户隐私的一个例子可以在《欧盟关于数据保护的规定》第 37 条中找到。[668] 不过，一些国家正通过实施法律限制来应对匿名通信的挑战[669] — 例如，意大利要求公共国际互联网接入提供商在用户开始使用服务之前辨别其身份。[670]

这些措施旨在帮助执法机构识别犯罪嫌疑人，但它们易于被犯罪嫌疑人避开 — 作案者可以使用来自无需注册国家的、未受保护的无线网络或者 SIM 卡。目前尚不明确的是，在网络安全战略中，对匿名通信和匿名接入国际互联网的限制是否应该发挥更加重要的作用。[671]

3.2.13 加密技术

另一个可使网络犯罪调查变得复杂的因素是加密技术，[672] 它使未获授权人员无法访问信息，是与网络犯罪作斗争过程中一种重要的技术解决方案。[673] 如同匿名通信和匿名接入，加密技术并不是什么新事物，[674] 但计算机技术改变了这一领域。如今，只需轻轻点击一下鼠标，就可以对计算机数据进行加密，使得执法机构难以破解密码和访问数据。[675] 尚不明确的是，违法者已经在多大程度上使用加密技术来掩盖其犯罪活动 — 例如，有报道指出，恐怖分子正在使用加密技术。[676] 一项关于儿童色情的调查表明，只有 6%的被抓获的儿童色情材料持有者使用了加密技术，[677] 但专家强调，在网络犯罪案件中，存在着越来越多使用加密技术的威胁。[678]

---

[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.

[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.

有一些工具可用来破解密码。[679] 有各种各样可用来保护用户文件免受非授权访问的软件产品。[680] 破解密码是可能的，但通常非常困难和缓慢 — 如果调查人员已经用过这些用来为文件加密的软件，那么也许能够拆开密码。[681] 作为选择，比如说，他们也许能够通过强力攻击来破解加密。[682]

取决于加密技术和密钥规模，要破解一个密码也许需要花费几十年的时间。[683] 例如，如果攻击者使用一个拥有 20 位密码的加密软件，那么密钥空间的规模大约为 100 万。使用当前每秒能够处理 100 万次操作的计算机，那么破解这一密码可以在不到 1 秒钟的时间内完成。不过，如果攻击者使用一个拥有 40 位密码的加密软件，那么可能需要花费两周的时间才能将其破解。[684] 如果攻击者使用 56 位的密码，那么单独一台计算机可能需要花费 2285 年的时间才能将其破解。如果攻击者使用 128 位的密码，那么即使有十亿个计算机系统单独运行，那么也需要花上数万亿年的时间才能将其破解。[685] 流行的最新版的加密软件 PGP，允许采用 1024 位密码。

当前的加密软件远不只仅对单个文件进行加密。例如，最新版的微软操作系统能够对整个硬盘进行加密。[686] 用户可以容易地安装加密软件。尽管某些计算机取证专家认为，这一功能并不会威胁到他们，[687] 但任何用户都可以广泛使用这一技术可能导致对加密技术的更广泛应用。还有一些工具可用来对通信进行加密 — 例如，电子邮件和电话呼叫 [688] 都可以使用 VoIP [689] 来发送。使用加密的 VoIP 技术，攻击者可以保护语音谈话免被截获。[690]

这些技术也可结合使用。运用软件工具，攻击者可以对消息进行加密，然后以图片或图像的形式交换它们 — 这种技术称为加密图形技术。[691] 对调查机构而言，难以区别究竟是无害的度假照片交换，还是带有加密、隐藏消息的图片交换。[692]

---

[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.

[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.

加密技术的可用性以及罪犯对加密技术的使用，对执法机构而言是一个挑战。解决这一问题的各种各样法律方法目前正在讨论中，[693] 包括：软件开发商为执法机构安装一个后门的潜在义务；限制密钥的强度；在犯罪调查情况下透露密钥的义务。[694] 但加密技术不仅仅可被攻击者使用 — 此类技术也可以以各种各样的方式用于法律目的。不恰当使用加密技术，可能难以对敏感信息实现保护。考虑到日益增多的攻击数量，[695] 自我保护是网络安全的一个重要因素。

3.2.14 小结

网络犯罪的调查与起诉对执法机构提出了诸多挑战。加强对与网络犯罪作斗争的人员的培训，以及起草适当而有效的法律，都至关重要。本小节逐一评述了在推动网络安全方面面临的重大挑战，并介绍证明现有手段力度不够、需要运用特殊手段的领域。

3.3 法律挑战

3.3.1 在起草国际刑法方面的挑战

适当的法律是调查和起诉网络犯罪的基础。不过，立法者必须持续对国际互联网的发展作出反应，并跟踪观察现有条款的有效性，特别是考虑到网络技术迅猛的发展速度时。

历史上，与计算机有关的服务或者与国际互联网有关的技术的引入，都会在技术引入后很快带来新的犯罪形式。计算机网络发展的一个例子是 20 世纪 70 年代 — 这之后不久，就出现了第一起未经授权访问计算机网络的案例。[696] 同样地，在 20 世纪 80 年代个人计算机引入后不久，就发生了第一起软件违法行为，当时，这些系统用于复制软件产品。

更新国家刑法以起诉新的在线网络犯罪形式需要花费时间 — 有些国家尚未结束这一调整过程。一直以来依据国家刑法来判定违法行为的罪行，这一作法需要进行评审和更新 — 例如，数字信息必须具备与传统签名和打印材料相当的效用。[697] 若不综合考虑与网络犯罪有关的违法行为，网络犯罪行为将无法受到起诉。

对国家刑法体系而言，主要的挑战是：意识到了潜在的新技术滥用与需要对国家刑法进行修改之间存在一个时延。这一挑战随着网络创新速度的加快，依然是相关和切题的。许多国家正致力于赶上法律调整的步伐。[698] 一般地，调整过程分为三个步骤：

---

[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.
[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.

调整国家法律必须首先意识到新技术的滥用问题。在国家执法机构内部，需要设立专门的部门，这些部门有资格来调查潜在的网络犯罪。成立计算机应急响应小组（CERT）、[699] 计算机事件响应小组（CIRT）、计算机安全事件响应小组（CSIRT）以及其他研究机构等，已改善了这一状况。

第二步是判断刑法的差距。为了确保有效的法律基础，有必要将国家法律中刑法条款的现状与应对新型犯罪活动的要求进行比较。在许多情况下，现有的法律都能够涵盖现有犯罪的各种变种（例如，针对伪造的法律也可以方便地用于电子文件）。法律修正的需求仅限于那些现有法律未能涵盖或者打击力度不够的违法行为。

第三步是起草新的法律。根据经验，由于网络技术的迅猛发展及其复杂的结构，如果不进行国际合作，要求国家主管部门起草完成针对网络犯罪的法律可能是困难的。[700] 各国单独起草网络犯罪法律可能导致巨大的复制效应，造成资源浪费，此外，起草机构也需要密切跟踪国际标准和战略的发展。没有国际上对各国刑法规定的协调，各国法律上的不一致性或不兼容性会使与跨国网络犯罪的斗争变得异常困难。因此，协调不同国家刑法的国际努力正变得日益重要。[701] 国家法律可以极大地受益于其他国家的经验和国际专家的法律建议。

3.3.2 新的违法行为

在大多数情况下，使用信息通信技术实施的犯罪并非新鲜事物，但经过修改的骗局将在网上实施。其中一个例子是欺诈 — 攻击者向受害者写信，意在误导受害者，与出于同样目的向受害者发送电子邮件，本质上没有太大区别。[702] 如果欺诈已经认定是一种犯罪行为，那么为起诉此类行为就不一定非要对国家法律进行调整。

但如果实施的行为是现有的法律中没有提及的，那么情况就不一样了。过去，一些国家针对普通的欺诈行为已经制定了适当的法律规定，但无法应对影响计算机系统而不影响人的欺诈行为。对这些国家而言，除了普通的欺诈案件之外，有必要采用新的法律来对与计算机有关的罪行进行判定。各种各样的案例表明，无论对现有的法律规定做多么广泛的解释，也无法替代采用新的法律。

除了针对臭名昭著的骗局对法律进行修改之外，立法者还必须不断地对新的和发展中的网络犯罪类型进行分析，以确保能对其罪行作出有效判定。在所有国家都尚未定罪的一个网络犯罪例子是，在计算机和在线游戏中的盗窃和欺诈。[703] 很长时间以来，关于在线游戏的讨论重点聚焦于未成年人的保护问题（例如，对年龄进行验证的要求）和非法内容（例如，在在线游戏“Second Life”中对儿童色情内容的访问）。[704] 新的犯罪行为仍在不断涌现 — 在线游戏中的虚拟货币也可能被“偷盗”，并在拍卖平台中进行交易。[705] 有些虚拟货币比照现实货币具有一定的价值（根据交易率），这给网络犯罪增加了“真实感”。[706] 此类违法行为可能不会在所有国家遭到起诉。为了防止违法者

[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.
[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/.

找到安全的避风港，密切关注世界范围的发展状况是至关重要的。

3.3.3 越来越多的信息通信技术的应用与新的调查手段的需求

在准备和实施其违法行为过程中，违法者以各种各样的方式来使用信息通信技术。[707] 执法机构需要适当的手段来调查潜在的犯罪行为。有些手段（如数据保留 [708] ）可能侵犯到清白的国际互联网用户的权利。[709] 如果犯罪行为的严重程度与这种侵犯的程度不成比例，那么调查手段的使用可能就是非合理的或者是非法的。结果是，在许多国家，目前尚未引入能够改进网络犯罪调查工作的手段。

调查手段的引入总是在执法机构可取得的优势与对清白的国际互联网用户权利的侵犯之间进行权衡的结果。监控正在进行的犯罪活动，以评估是否要改变威胁等级，是至关重要的。通常，新手段的引入已经在“与恐怖主义作斗争”的基础上被证明是合理的，但这是一种更为深远的动机，而不仅仅只是一种特殊的理由。

3.3.4 开发数字证据程序

特别是由于相比保存物理文件而言，低得多的成本，[710] 因此数字文件的数量正与日俱增。[711] 数字化和信息通信技术的新兴应用，对与证据收集及其在法庭上使用有关的程序产生了巨大影响。[712] 发展的一个结果是，引入数字证据作为一种新的证据源。[713] 它被定义为使用计算机技术存储或传输的任何数据，用于支持推测一种违法行为是如何产生的。[714] 对数字证据的处理也伴随着一些独特的挑战，并需要特定的程序。[715] 其中最难的一个问题是保持数字证据的完整性。[716] 数字数据是极为脆弱的，非常容易被删去 [717] 或被修改。对保存在系统存储器 RAM 中的信息而言更是如此，当系统关机时，这些信息会被自动删去，[718] 因此，需要特殊的保存技术。[719] 此外，新的发展对数字证据的处理产生了极大的影响。一个例子是云计算。过去，调查者能够重点关注犯罪嫌疑人的前提条件，并

[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.

[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.

搜寻计算机数据。如今，他们需要考虑这些数字信息可能保存在国外，并且必要的话，只能远程访问之。[720]

数字证据在网络犯罪调查的各个阶段都发挥着重要作用。一般可将数字证据处理分为四个阶段：[721]

- 识别相关的证据；[722]
- 收集和保留证据；[723]
- 分析计算机技术和数字证据；以及
- 在法庭上出示证据。

除了涉及在法庭上出示证据的相关程序，收集数字证据的方法需要特别加以关注。数字证据的收集与计算机取证相关联。“计算机取证”这一术语指的是，本着搜索数字证据的目的，对信息技术设备进行系统的分析。[724] 对于以数字格式保存的数据仍在不断增长这一事实，则突显了此类调查面临的逻辑上的挑战。[725] 除了手工调查之外，自动执行取证程序的方法发挥着重要作用，[726] 例如，使用基于散列值的方法来搜索已知的儿童色情图片，[727] 或者借助关键字进行搜索。[728]

例如，取决于特殊调查的要求，计算机取证可以包括以下步骤：

- 分析嫌疑犯所用的硬件和软件；[729]
- 在确定相关证据中为调查者提供支持；[730]
- 恢复被删除的文件；[731]
- 破解文件；[732] 以及
- 通过分析通信流量数据来识别国际互联网用户。[733]

---

[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.
[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.

4. 反网络犯罪战略

认可的网络犯罪数量与日俱增，同时，用于自动执行网络犯罪活动的技术工具数量（包括匿名的文件共享系统[734]以及设计用于开发计算机病毒的软件产品[735]）也愈来愈多，意味着与网络犯罪作斗争已经成为全世界执法活动的重要组成部分。网络犯罪无论在发达国家还是在发达国家，都是一个挑战。由于信息通信技术发展极为迅速，特别是在发展中国家的发展更是迅速，因此，建立和实施一种有效的反网络犯罪战略，作为国家网络安全战略的一部分，是一项极为重要的工作。

4.1 将网络犯罪立法作为网络安全战略的一部分

正如之前所指出的那样，网络安全[736]在当前信息技术以及国际互联网服务的发展过程中起着重要作用。[737]使国际互联网更安全（以及保护国际互联网用户），已经成为发展新业务以及政府政策的一个有机组成部分。[738]网络安全战略 — 例如，技术保护系统的发展或者对用户进行教育，以防止成为网络犯罪的受害者 — 将有助于降低网络犯罪的风险。[739]

---

[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.

[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.

反网络犯罪战略应当成为网络安全战略的一个有机组成部分。国际电联的《全球网络安全议程》[740] 是一个全球性的对话和国际合作框架，旨在协调国际社会应对日益严峻之网络安全挑战的响应行动，并增强信息社会的信心和安全，《议程》建立在现有的工作、倡议和合作关系基础之上，目标是提议制定一些全球战略，以应对这些相关的挑战。在《全球网络安全议程》五大支柱中所强调的所有必需的措施，都与任何一种网络安全战略相关。此外，为了有效地与网络犯罪开展斗争，要求采取在这所有五大支柱中所提出的各项措施。[741]

4.2 现有战略的实施

一种可能性是，将在工业化国家中制定的反网络犯罪战略引入到发展中国家中，这既可以降低成本，也可以节省时间。对现有战略的实施可使发展中国家受益于现有的见识和经验。

尽管这样，对现有反网络犯罪战略的实施也存在许多困难。尽管发展中国家和发达国家都面临类似的挑战，但可采用的最佳解决方案还将取决于各个国家的资源与能力。工业化国家也许能够以不同的和更加灵活的方式来推动网络安全 — 例如，通过着眼于所需成本更高的技术保护问题。

采用现有反网络犯罪战略的发展中国家还需要考虑到其他几个问题：

- 与各个法律体系的兼容性；
- 支持倡议的状况（如社会的教育水平）；
- 自我保护措施采用的程度；以及
- 私营部门支持的程度（如通过公－私合作关系来支持）等。

4.3 区域差异

鉴于网络犯罪的国际特性，协调好各国的法律和技术，对与网络犯罪作斗争而言至关重要。不过，协调工作必须考虑到不同的区域需求与能力。许多法律和技术标准得到了工业化国家的认可，但并没有包含对发展中国家而言是重要的各方面问题，这一事实突显了在实施反网络犯罪战略时考虑到区域方面问题的重要性。[742] 因此，当在其他区域实时这些法律和技术标准时，需要考虑到区域因素和差异。

[740] For more information see: http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.
[741] See below: Chapter 4.4.
[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.

4.4 网络安全支柱内网络犯罪问题的关联性

《全球网络安全议程》有七大目标，建立在五大工作领域之上：1）法律措施；2）技术和程序措施；3）组织结构；4）能力建设；以及 5）国际合作。如上所述，与网络犯罪相关的问题在《全球网络安全议程》所有五大支柱中起着重要作用。在这些工作领域，法律措施着重于如何应对经由信息通信技术网络、以一种国际兼容方式实施的犯罪行为所带来的法律挑战。

4.4.1 法律措施

在五大支柱内，法律措施可能是与反网络犯罪战略最为相关的。这首先要求所有必要的实体刑法条款来对以下犯罪行为定罪，如计算机欺诈、非法访问、数据干扰、侵犯版权以及儿童色情等。[743] 事实是，刑法中适用于在网络之外实施的、类似的犯罪行为的现有条款，并不一定就适用于经由国际互联网实施的犯罪。[744] 因此，在判断任何可能的差距时，对当前各国的法律进行一次全面的分析是非常必要的。[745] 除了实体刑法的条款，[746] 执法机构还需要一些调查网络犯罪的必要工具和手段。[747] 此类调查本身就面临诸多挑战。[748] 作案者几乎可以从世界任何地方实施犯罪，并采取措施掩盖其身份。[749] 与那些用于调查普通犯罪案件的工具和手段相比，调查网络犯罪所需的工具和手段可能完全不同。[750] 由于网络犯罪的国际特性 [751]，因此，还有必要制定一个国家法律框架，以便能够与国外的执法机构携手合作。[752]

4.4.2 技术与程序措施

与网络犯罪有关的调查常常具有很强的技术性。[753] 除了在调查期间需要维护证据的完整性之外，还需要严密的程序。因此，提升必需的能力以及制定必要的程序，是与网络犯罪作斗争的一项必然要求。

---

[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.
[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/jrnl/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-

另一个问题是发展技术保护系统。良好保护的计算机系统更难攻击。通过实施适当的安全标准来完善技术保护是重要的第一步。例如，修改在线银行系统（例如从 TAN [754] 转为 ITAN [755]），就可大大消除当前“网络钓鱼”攻击带来的风险，这充分展示了技术解决方案的极端重要性。[756] 技术保护措施应包括技术基础设施的所有要素 — 核心网络基础设施以及世界范围内众多单独相连的计算机。为了保护国际互联网用户和企业，可以确定两个潜在的目标群：

- 最终用户和企业（直接方法）；以及
- 服务提供商和软件公司。

逻辑上，它着重于保护核心基础设施（如骨干网络、路由器、重要的服务等），比起将数百万个用户融入到反网络犯罪战略中来，这要相对容易一些。对用户的保护可以通过确保消费者使用的服务（如在线银行）的安全来间接进行。这种间接保护国际互联网用户的方法可以减少需要包含在各提升技术保护环节中的人员与机构数量。

尽管限制需要包含在技术保护措施中的人员数量看起来是理想的，但计算机和国际互联网用户常常是网络安全中最薄弱的环节，是作案者的主要目标。相比攻击金融机构中受到良好保护的计算机系统，攻击个人计算机来获取敏感数据通常要容易一些。尽管存在这些逻辑问题，但保护好最终用户的基础设施对做好整个网络的技术保护而言是至关重要的。

国际互联网服务提供商和产品供应商（如软件公司）在支持反网络犯罪战略中起着非常重要的作用。由于他们直接与客户接触，因此他们可以扮演安全行为保证人的角色（例如，分发针对最新欺骗诡计的保护工具并提供相关信息）。[757]

4.4.3 组织结构

为了有效开展与网络犯罪的斗争，需要具备高度完善的组织结构。如果没有避免重叠、分工明确的适当的组织结构，那么几乎无法完成复杂的、需要不同法律和技术专家援助的网络犯罪调查。

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.

[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/.

4.4.4 能力建设与用户教育

网络犯罪是一种全球现象。为了能够有效开展对违法行为的调查，需要协调各国的法律，并需制定一些方法来开展国际合作。为了确保在发达国家和发展中国家中建立统一的全球标准，开展能力建设是必要的。[758]

除了能力建设，还需要开展用户教育。[759] 某些网络犯罪 — 特别是那些涉及欺诈的犯罪，如“网络钓鱼”和“电子欺骗”等 — 通常并非因为缺乏技术保护措施，而是因为受害者缺乏保护意识。[760] 有各种各样的软件产品可以自动识别伪冒的网站，[761] 但到目前为止，这些产品无法识别所有可疑的网站。仅仅基于软件产品的用户保护策略，将大大限制保护好用户的能力。[762] 尽管技术保护措施仍在继续发展，而且可用的产品也在定期更新，但这些产品仍不能替代其他方法。

防止网络犯罪的最重要因素之一是用户教育。[763] 例如，如果用户知道为其提供服务的金融机构绝不会通过要求提供密码或银行账号详细信息的电子邮件联系他们，那么他们就不会成为网络钓鱼的受害者，或者可以识别欺骗攻击。对国际互联网用户的教育可减少攻击者潜在攻击目标的数量。对用户的教育可以通过以下方法进行：

- 公共活动；
- 学校、图书馆、信息技术中心和大学中的课程；
- 公共－私人合作关系（PPP）。

对用户进行有效教育和制定信息战略的一项重要要求是公开最新的网络犯罪威胁。一些国家和/或私营企业为了避免客户对其在线通信服务失去信任，拒绝承认其公民与客户分别受到了网络犯罪威胁的影响。美国联邦调查局曾明确要求各公司克服其厌恶负面宣传的心理，如实报告网络犯罪威胁情况。[764] 为了确定威胁等级，也为了告知用户，改进对相关信息的收集和公布是一项非常重要的工作。[765]

---

[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.

[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

4.4.5 国际合作

在许多情况下，国际互联网中的数据传送过程会影响到多个国家。[766] 这是网络设计的必然结果，也是出于以下事实：即使数据传送的直接线路临时受阻，协议也可确保传输能够成功进行。[767] 此外，大量的国际互联网服务（如托管服务等）是由国外的公司来提供的。[768]

在这些情形中，违法者与受害者并非同处在一个国家中，而对网络犯罪调查来说，需要所有受影响国家的执法机构开展合作。[769] 如果未获得相关国家主管部门的同意，是很难进行国际和跨国调查的，因为这涉及国家主权原则。这项原则一般不允许某个国家在未经当地主管部门许可的情况下在他国范围内进行调查。[770] 因此，开展国际和跨国网络犯罪调查需要得到所有相关国家当局的支持。在大多数情况下，成功的网络犯罪调查只有一个很短的时间间隙，考虑到这一事实，当面对网络犯罪调查时，运用传统的相互法律援助体系就会面临一些明显的困难，原因是相互法律援助通常要求履行一些费时的正式程序。因此，强化和改善国际合作将在网络安全战略以及反网络犯罪战略的制定与实施中发挥重要而关键的作用。

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.

[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. 国际法律方法概述

本章将对国际法律方法[771]以及与国家法律方法之间的关系做一概述。

5.1 国际方法

许多国际组织不断致力于分析网络犯罪的最新进展，并建立了一些工作小组，以制定与这些犯罪活动作斗争的策略。

5.1.1 八国集团[772]

1997 年，八国集团（G8）建立了涉及与网络犯罪作斗争[773]的“高科技犯罪分委员会”。[774]八国集团的司法与内政部长在美国华盛顿举行峰会期间，批准了用于与高科技犯罪作斗争的《十条原则》以及《十点行动计划》。[775]随后，八国集团首脑签署了这些原则，它们包括：

- 不应存在任何庇护滥用信息技术罪犯的安全避风港。
- 对国际高科技犯罪的调查与起诉必须在所有相关国家中协调进行，不管这些国家是否受到损害。
- 执法人员必须接受培训，并且配备应对高科技犯罪的装备。

1999 年，在俄罗斯联邦首都莫斯科举行的、关于打击跨国有组织犯罪部长级会议上，八国集团详细说明了其在与高科技犯罪作斗争方面的规划。[776]它们表达了对跨国有组织犯罪（如儿童色情等）、交易的可跟踪性以及越境访问所储存数据等问题的关注。会议公报包含了许多与网络犯罪作斗争方面的原则，成为了许多国际战略的基础和依据。[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

专家小组已经实现的实际工作成果之一是提出了 24/7－国际联络网络，要求各参与国为跨国调查建立联络点，联络点每周 7 天、每天 24 小时都处于运行状态。[778]

2000 年，在法国巴黎的八国集团大会上，八国集团提出了网络犯罪的议题，并呼吁各国防止存在非法的数字避风港。当时，八国集团已经将其寻求国际解决方案的努力与《欧洲理事会关于网络犯罪的公约》结合起来。[779] 2001 年，在日本东京举行的研讨会上，[780] 八国集团讨论了与网络犯罪作斗争的程序手段，焦点在是应当履行数据保留义务，还是将数据保留作为一种替代解决方案。[781]

---

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

2004 年，八国集团司法和内政部长会议发表了一份公报，在公报中提出了在与使用国际互联网的犯罪作斗争时，需要建设全球性的能力。[782] 八国集团再次提到了《欧洲理事会关于网络犯罪的公约》。[783]

在 2006 年莫斯科会议期间，八国集团司法和内政部长们讨论了与与网络犯罪作斗争有关的问题以及网络空间问题，并特别提到需要改进有效的措施。[784] 八国集团司法和内政部长会议之后召开了八国集团莫斯科峰会，会议讨论了有关网络恐怖主义 [785] 的议题。[786]

2007 年，在德国慕尼黑举行的八国集团司法和内政部长会议期间，进一步讨论了恐怖分子使用国际互联网的问题，与会各国同意对恐怖组织滥用国际互联网的行为予以定罪。[787] 该协议未将各国应予定罪的某些特定行为包括在内。

5.1.2 联合国 [788]

在第 8 届预防犯罪和罪犯待遇问题大会上（于 1990 年 8 月 27 日至 9 月 7 日在古巴哈瓦那举行），联合国大会批准了一项涉及计算机犯罪立法问题的决议。[789] 根据其第 45/121（1990）号决议，联合国于 1994 年发布了一份关于预防和控制与计算机有关的犯罪的手册。[790]

---

activities can find all the facilities they need, including financial ones, for laundering the product of their crimes. Since we must 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 at http://www.uncjin.org/Documents/EighthCongress.html.

2000 年，联合国大会批准了一个关于与滥用信息技术犯罪行为作斗争的决议，它与八国集团在 1997 年通过的《十点行动计划》有许多相似之处。[791] 在该决议中，联合国大会确定了一系列防止滥用信息技术的措施，包括：

> 各国应确保本国法律和作法不会为滥用信息技术进行犯罪活动的人提供“安全避风港”；
>
> 在调查与起诉滥用信息技术的国际案件中开展执法合作，应在所有相关国家中协调进行；
>
> 执法人员应接受培训，并配备应对滥用信息技术犯罪行为的装备；

2002 年，联合国大会批准了另一个关于与滥用信息技术犯罪行为作斗争的决议。[792] 该决议参考了现有的与网络犯罪作斗争的国际方法，并强调指出了一系列解决方案。

> 注意到国际与区域组织在与高科技犯罪作斗争的努力，包括欧洲理事会在详细制定《网络犯罪公约》方面的工作，以及那些致力于在政府与私营部门之间就网络空间安全与信心推动对话的组织的工作，
>
> 1. 在制定国家法律、政策和完善作法以便与滥用信息技术犯罪行为作斗争的过程中，要求各成员国在适当时考虑到预防犯罪和刑事司法委员会以及其他国际和地区组织的工作和取得的成就；
>
> 2. 注意到在其 55/63 号决议中所述之各种措施的价值，再次要求各成员国在其与滥用信息技术犯罪行为作斗争的过程中考虑到这些措施；
>
> 3. 决定暂缓考虑这一主题，即预防犯罪和刑事司法委员会在针对高科技犯罪和与计算机有关的犯罪的行动计划中所展望的待定工作。

2004 年，联合国成立了一个应对垃圾邮件、网络犯罪和其他涉及国际互联网主题的工作小组，强调了联合国有兴趣参与当前国际上有关网络犯罪威胁的讨论。[793]

2005 年，在泰国曼谷举行的关于预防犯罪和刑事司法的第 11 次联合国大会上，联合国发表了一份声明，强调在与网络犯罪作斗争过程中需要做好协调。[794] 声明强调了以下问题：

> 我们重申在犯罪问题上运用现有工具以及进一步开发国家措施和开展国际合作的重要性，如考虑强化和加大各种措施的力度，尤其是加强对网络犯罪、洗钱和文化产品非法贩卖的打击力度，以及就引渡、相互法律援助以及没收、回收和返还犯罪收益等开展合作。
>
> 我们注意到，处在当前全球化的时代，伴随着信息技术和新的电信与计算机网络系统的迅猛发展，出现了将这些技术滥用于犯罪目的的现象。因此，我们欢迎各国强化和补充

[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.

现有的合作，推动对高科技犯罪和与计算机有关的犯罪的调查与起诉，包括与私营部门的合作关系。我们认识到联合国对有关打击网络犯罪的区域和其他国际论坛的重要贡献，要求预防犯罪和刑事司法委员会考虑到它的经验，检验在联合国和其他同样关注这些问题的组织的共同领导下为该领域提供进一步援助的可行性。

此外，联合国系统的大量《决定》、《决议》和《建议》都提到了与网络犯罪有关的问题。最重要的一些问题包括：

- 联合国毒品和犯罪问题办公室（UNODC）预防犯罪和刑事司法委员会，[795] 批准了一个关于在与儿童性侵犯犯罪活动作斗争过程中有效预防犯罪和刑事司法响应的决议。[796]
- 2004 年，联合国经济和社会理事会 [797] 批准了一个关于在预防、调查、起诉和惩治欺诈、非法滥用和伪造身份及其相关犯罪活动中开展国际合作的决议。[798] 2007 年，该理事会又批准了一个关于在预防、调查、起诉和惩治经济诈骗及与身份有关的犯罪活动中开展国际合作的决议。[799] 两个决议都没有明确描述该如何应对与国际互联网有关的犯罪行为，[800] 但同样适用于这些犯罪行为。

2004 年，该理事会批准了一个关于借助国际互联网销售合法药品的决议，它被明确视为一种与计算机犯罪有关的现象。[801]

5.1.3 国际电信联盟 [802]

作为联合国的一个专门机构，国际电信联盟（ITU）在电信标准化和发展以及网络安全问题方面起着领导作用。在其他活动中，国际电联也是信息社会世界峰会（WSIS）的领导机构，该峰会分两个阶段进行，2003 年在瑞士的日内瓦市，2005 年在突尼斯的突尼斯市。来自世界各国的政府代表、政策制定者和专家就如何最好地应对全球信息社会发展带来的一系列问题交换了意见和经验，包括制定兼容的标准与法律。峰会的结果包含在《日内瓦原则声明》《日内瓦行动计划》、《突尼斯承诺》以及《突尼斯信息社会议程》中。

《日内瓦行动计划》强调了采取与网络犯罪斗争的措施的重要性：[803]

[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.

[803] WSIS Geneva Plan of Action, 2003, available at: http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

***C5.* 树立使用信息通信技术的信心并确保使用的安全**

***12.* 信心与安全是信息社会的重要支柱。**

b) 政府应当与私营部门合作，来防止、探测并响应网络犯罪和信息通信技术滥用现象，方法包括：制定指南，以便将各国在这些领域正在进行的工作考虑在内；考虑立法，以便对滥用行为进行有效的调查和起诉；促进有效的相互援助；在国际层面上加强制度支持，以便防止、探测和恢复此类事件；同时，鼓励对用户进行教育，提高其意识。

2005 年在突尼斯召开的信息社会世界峰会第二阶段会议也提到了网络犯罪问题。《信息社会突尼斯议程》[804] 强调，在与网络犯罪作斗争的过程中需要开展国际合作，并参考现有的法律方法，如《联合国大会决议》以及《欧洲理事会关于网络犯罪的公约》等：

40. 我们强调对网络犯罪进行起诉的重要性，包括在某个司法管辖地实施网络犯罪而影响到另一个司法管辖地的情形。我们进一步强调，在国家和国际层面上采取高效、有效的工具和行动的必要性，以促进有关网络犯罪的执法机构之间的国际合作。我们号召各国政府与其他相关利益方密切合作，制定必要的法律来调查和起诉网络犯罪，并注意到了现有的框架，如联合国大会关于“与非法滥用信息技术行为作斗争”的 55/63 和 56/121 号决议以及区域性倡议，包括但不限于欧洲理事会的《网络犯罪公约》。

作为信息社会世界峰会的一项成果，国际电联被指定为行动线 C5 的唯一促进机构，致力于树立使用信息通信技术的信心，并保证其安全。[805] 在 2007 年召开的信息社会世界峰会行动线 C5 第二次促进会议上，国际电联秘书长强调了在与网络犯罪作斗争的过程中开展国际合作的重要性，并宣布发布《国际电信联盟全球网络安全议程》。[806] 《全球网络安全议程》由七大目标组成，[807] 建立在五大战略支柱基础之上，[808] 包括为网络犯罪示范法的制定而精心制作的战略。这七大目标是：

1 为制定模式网络犯罪法律而精心确定战略，所制定的法律可全球通用，并能与现有的国家和区域法律措施互操作。

2 为创建针对网络犯罪的适当的国家和区域组织结构和政策而精心制定战略。

3 为建立全球可接受的、针对软件应用程序和系统的最低安全标准和认证计划而精心制定战略。

4 为建立用于监控、告警和事件响应的全球框架而精心制定战略，以确保在新的与现有的举措之间能够实现跨国协调。

[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.

5 为创建与批准普通的和通用的数字身份系统以及必要的组织结构而制定战略，以确保能够识别出国之人的数字证书。

6 为促进人与机构的能力建设而制定全球战略，以增强部门间以及所有上述领域中的知识与技能。

7 为实现所有上述领域中的国际合作、对话和协调，建议为全球利益相关各方战略构建一个可能的框架。

成立了一个专家小组，来制定与 GCA 有关的战略。[809]

5.1.4 欧洲理事会[810]

1976 年，欧洲理事会（CoE）强调指出了与计算机有关的犯罪的国际特点，并且在一次涉及经济犯罪问题的会议上讨论了这一主题。自那以后，这一主题就排上了欧洲理事会的议事日程。[811] 1985 年，欧洲理事会任命了一个专家委员会，[812] 来讨论计算机犯罪的法律方面问题。[813] 1989 年，欧洲犯罪问题委员会批准了“关于与计算机有关的犯罪的专家报告”，[814] 报告对与新型电子犯罪（包括计算机欺诈和伪造）作斗争所需的实体刑法进行了分析。1989 年，部长委员会批准了一份建议书，[815] 建议书特别强调了计算机犯罪的国际特点：

根据《欧洲理事会规约》第 15.b 条的规定，部长委员会考虑到，欧洲理事会的目标是实现各成员国之间的更加紧密的团结；

意识到对与计算机有关的犯罪的新挑战作出适当而迅速反应的重要性；考虑到与计算机有关的犯罪常常具有跨国特点；意识到因此而需要进一步协调各国的法律和作法，并且为了促进国际法律合作，建议各成员国的政府：

1．在评审本国的法律或者进行新的立法时，考虑到关于与计算机有关的犯罪的报告（此报告由欧洲犯罪问题委员会精心制作），尤其是要考虑到其中有关国家立法的指导方针；

2．向欧洲理事会秘书长报告本国在 1993 年期间在与计算机有关的犯罪方面的任何法律、司法实践的进展情况以及国际法律合作的经验。

1995 年，部长委员会批准了另一份建议书，此建议书涉及因跨国计算机犯罪而导致的各种问题。[816] 在建议书的附录中概述了有关起草适当法律的指导方针。[817]

---

[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.
[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.

1996 年，欧洲犯罪问题委员会（CDPC）决定成立一个用于应对网络犯罪问题的专家委员会。[818]在建立专家委员会之时，提出了超出另一份建议书并其超一份《公约》的主意。[819] 1998 和 2000 年间，该委员会举行了 10 次全体会议、15 次开放起草小组会议。在 2001 年 4 月召开的委员会全体会议第二阶段会议上，大会批准了《公约》草案。[820] 最终定稿的《公约》草案提交 CDPC 批准，随后，《公约》草案文本提交给了部长委员会，以便批准和签署。2001 年 11 月 23 日，在布达佩斯举行的签字仪式上，开始签署《公约》，共有 30 个国家签署了这一《公约》（包括四个非欧洲理事会成员国，即美国、加拿大、日本和南非，它们参与了谈判）。到 2009 年 4 月，共有 46 个国家 [821] 签署了《公约》，并有 25 个国家[822] 批准了[823]《网络犯罪公约》。一些国家，如阿根廷、[824] 巴基斯坦、[825] 菲律宾、[826] 埃及、[827] 博茨瓦纳 [828] 和尼日利亚 [829] 等，已经依照《公约》起草了本国法律。尽管这些国家尚未签署该《公约》，但它们支持《公约》起草者所指的法律协调和标准化过程。如今，《公约》被视为与网络犯罪作斗争的一种重要的国际手段，得到了不同国际组织的支持。[830]

[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, 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

《公约》出台后，紧接着出台了《网络犯罪公约第一附加协议》。[831] 在对《公约》文本进行谈判的过程中，对种族主义以及排外材料散布行为的定罪问题成了一个有争议的话题。[832] 有些国家对言论自由原则采取严格保护，[833] 它们表达了自己的担心，即如果《公约》中包含的规定有悖其言论自由原则，那么它们可能无法签署《公约》。[834] 因此，这些问题被整合到了一份独立的协议中。到2008 年 10 月，已有 20 个国家[835] 签署、13 个国家 [836] 批准了《附加协议》。

2007 年，欧洲理事会为了加强对未成年人遭受性侵犯的保护，引入了一份新的《公约》。[837] 在关于保护儿童的《公约》公开签署的第一天，就在 23 个国家签署。[838]《公约》的一个重要目标就是协调各国旨在保护儿童免遭性侵犯的刑法条款。[839] 为现实这一目标，公约包含了一组刑法条款。除了针对儿童性虐待的判罪（第 18 条），公约还包含涉及儿童色情内容交换（第 20 条）和出于性目的对儿童进行教唆（第 23 条）的法律条款。

5.2 区域方法

除了面向全球的国际组织之外，还有大量关注特定区域的国际组织也在着力解决与网络犯罪有关的问题。

5.2.1 欧盟 [840]

在刑法领域的立法方面，欧盟的权力是有限的。[841] 它只能在一些特定领域协调国家刑法，如对欧盟经济利益的保护以及网络犯罪等。[842]

---

[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.

[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.

1999 年，通过批准欧洲委员会的通讯《电子欧洲 — 服务于所有人的信息社会》[843]，欧盟提出了“电子欧洲”的倡议。2000 年，欧洲理事会批准了全面的《电子欧洲行动计划》，并呼吁各国在 2002 年底之前实施这一行动计划。

2001 年，欧洲委员会发表了一份名为《改善信息基础设施安全与计算机相关犯罪作斗争，创造更加安全的信息社会》的通讯。[844] 在该通讯中，欧洲委员会分析并论述了网络犯罪问题，并指出，需要采取有效措施来应对信息系统和网络所面临的完整性、可用性与可信任性方面的威胁。

> 信息和通信基础设施已经成为我们经济中不可或缺的重要组成部分。遗憾的是，这些设施本身具有弱点，为犯罪分子实施犯罪活动提供了新的机会。这些犯罪活动可能采取多种多样的形式，并可能跨越多个国家。尽管出于种种原因，没有这方面的可靠统计数据，但毫无疑问，这些犯罪活动已经对行业投资和资产构成了威胁，也对信息社会的安全和信心构成了威胁。最近报告的有关拒绝服务攻击和病毒攻击的一些例子，已造成巨大的经济损失。
>
> 通过强化信息基础设施的安全性，以及通过确保执法机构拥有适当的执法手段，仍有机会来阻止犯罪活动，并同时充分尊重个人的基本权利。[845]
>
> 委员会参与了欧洲理事会（CoE）和八国集团（G8）的讨论，认识到与程序法问题有关的复杂性和难度。但是，欧盟内部就与网络犯罪作斗争开展有效合作，是构建一个更加安全的信息社会并将网络世界建设成为一个自由、安全和公正的领地的至关重要的因素。[846]
>
> 委员会将根据 TEU 的标题 VI 提出一些立法建议。
>
> [...]以便进一步在高科技犯罪领域接近实体刑法。这将包括那些涉及黑客攻击和拒绝服务攻击的违法行为。委员会还将详细审视旨在打击国际互联网上种族主义和排外行为的行动的范围，为的是依据 TEU 标题 VI，提出一个涵盖离线和在线种族主义和排外行为的框架决定。最后，还要审视国际互联网上非法药物的问题。[847]
>
> 委员会将继续充分发挥作用，确保在其他国际论坛的各成员国间做好协调，这些国际论坛正对网络犯罪问题进行讨论，如欧洲理事会和八国集团等。在欧盟层面上，委员会的

[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.
[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.

倡议将充分考虑其他国际论坛的进展情况，同时积极寻求进一步拉近欧盟内部的距离。[848]

另外，2001 年，委员会发表了一篇关于“网络和信息社会”的通讯，[849] 对网络安全问题进行了分析，并为在该领域采取的行动起草了一份战略纲要。

委员会的这两篇通讯都强调了需要在欧盟内部使各国的实体刑法更接近 — 尤其当考虑到针对信息系统的攻击。在与网络犯罪作斗争过程中，在欧盟内部对实体刑法进行协调被认为是在欧盟层面上所有举措的一个关键要素。[850] 根据这一战略，2002 年 [851]，委员会提出了一份有关“关于信息系统攻击的框架决定”的提议。委员会的提议经过局部修改，最终被理事会批准。[852]

该框架决定关注《欧洲理事会关于网络犯罪的公约》，[853] 但重点是协调实体刑法的规定，旨在保护基础设施各要素。

第 2 条 — 非法访问信息系统

1．各成员国应采取必要的措施，确保未经授权地有意访问整个或部分信息系统是一种可给处罚的犯罪行为，至少对违法者是非未成年人的案件而言是这样的。

2．各成员国可以决定，对第 1 段中提到的行为，只有在破坏安全措施的情况下来实施时，才可判为罪。可以通过有效的、成比例的和劝诫性的刑罚来处罚。

第 3 条 — 非法系统干扰

各成员国应采取必要的措施，确保未经授权地通过输入、传输、损害、删除、破坏、更改、隐瞒或者造成无法访问计算机数据的手段来有意严重阻碍或中断信息系统功能发挥的行为是一种可处罚的犯罪行为，至少对违法者是非未成年人的案件而言是这样的。

第 4 条 — 非法数据干扰

各成员国应采取必要的措施，确保未经授权地有意删除、损害、破坏、更改、隐瞒或者造成无法访问信息系统中的计算机数据的行为是一种可处罚的犯罪行为，至少对违法者是非未成年人的案件而言是这样的。

2005 年，欧共体法院声明，通过刑法的 [854]、关于保护环境的理事会框架决定是不合法的。[855] 有了这一决定，欧共体法院澄清了关于刑法条款的第一支柱和第三支柱之间的权力分配问题。它决

[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.”
[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.

定，通过刑法的、关于保护环境的框架决定是不可分割的，违反了欧盟第 47 条，原因是它侵犯了欧共体第 175 条赋予欧共体的权力。[856] 在一篇关于欧共体法院决定的通讯中，[857] 委员会声明：

> “从主题的角度来看，除了环境保护之外，欧洲法院的推理可以适用于任何欧共体的政策和自由，它们涉及具有约束力的法律，应将刑罚与这些法律关联起来，从而确保它们的有效性。”

委员会声明，根据欧共体法院的判断，许多涉及刑法的框架决定是完全或部分不正确的，原因是其中的所有或部分条款是在错误的法律基础上被批准的。在修正版的通讯中明确提到了关于信息系统攻击的框架决定。

刑事程序法方面的问题 — 尤其是协调调查和起诉网络犯罪所需的法律手段问题 — 未并入框架决定中。不过，2005 年，委员会为一份涉及数据保留的欧盟指令起草了一份提议。只在提交欧洲议会三个月后，理事会就批准了这一提议。[858] 《指令》的关键要素是国际互联网服务提供商有义务保存特定的通信流量数据，这些数据对于识别网络空间中的违法犯罪人员是必不可少的。

> **第 3 条 — 数据保留的义务**
>
> 1．为了部分废除 2002/58/EC 指令第 5 条、第 6 条和第 9 条，各成员国应采取一些措施来确保本指令第 5 条中规定的数据能够依照其条款的规定得以保留，所保留的数据指的是：由公众可用的电子通信服务提供商或者公共通信网络，在其管辖范围内、在提供有关通信服务时，产生或处理的数据。
>
> 2．第 1 段中规定的保留数据的义务应包括保留第 5 条中规定的数据，它们与不成功的呼叫尝试有关，在这些呼叫尝试中，由公众可用的电子通信服务提供商或者公共通信网络，在其管辖范围内、在提供有关通信服务时，产生或处理以及保存（关于电话数据）或记录（关于国际互联网数据）了这些数据。《指令》不得要求保留与未连接呼叫有关的数据。

指令将涵盖国际互联网上有关任何通信的关键信息这一事实，招致了人权组织的强烈批评，并可能导致对指令进行评审，将由立宪法院来实施评审。[859]

2007 年，委员会发表了一篇有关与网络犯罪作斗争的一般政策的通讯。[860] 通讯概述了当前状况，强调了《欧洲理事会关于网络犯罪的公约》作为在与网络犯罪作斗争过程中主导国际手段的重要性。另外，通讯还指出了委员会将在其未来活动中重点关注的问题。包括：

---

[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

[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.

- 加强在与网络犯罪作斗争过程中的国际合作；
- 为培训活动提供更好的财政支持；
- 组织一次执法专家的会议；
- 加强与行业的对话；
- 监控网络犯罪不断演变的威胁，以评估是否需要进一步立法。

2008 年，欧盟开始讨论《关于与恐怖主义作斗争的框架决定的修正案草案》。[861] 在草案修正案的引言中，欧盟强调指出，现有的法律框架对那些协助或者教唆和煽动恐怖主义的行为进行判罪，但并不对那些通过国际互联网散步恐怖主义技能的行为判罪。[862] 有了这一修正案，欧盟正在积极采取措施，缩小差距，使整个欧盟的法律更接近《欧洲理事会关于预防恐怖主义的公约》。

第 3 条 — 与恐怖活动相关的犯罪行为

1．出于本框架决定的目的：

(a) “公开煽动实施恐怖活动”意味着传播一条消息，或者使公众可以获得该消息，意在煽动人们实施第 1 条（1）（a）～（h）中所列举的某种行为，如果这种煽动行为发生，那么无论是直接地还是间接地鼓吹恐怖主义行为，都会导致一种或多种此类恐怖活动被实施的危险；

(b) “为恐怖主义招募人员”意味着教唆他人实施第 1 条（1）或第 2 条（2）中所列举的某种行为；

(c) “为恐怖主义培训人员”意味着提供如何制造或使用爆炸物、轻武器或其他武器或毒物或危险物质的指南，或者提供采用其他特定方法和技术的指南，目的是实施第 1 条（1）中所列举的某种行为，明知提供的这种技能是准备用于这种目的的。

2．各成员国须采取必要措施来确保与恐怖相关的犯罪行为包含以下故意的行为：

(a) 公开煽动实施恐怖活动；

(b) 为恐怖主义招募人员；

(c) 为恐怖主义培训人员；

(d) 本着实施第 1 条（1）中所列举的某种行为的目的而恶意盗窃；

(e) 本着实施第 1 条（1）中所列举的某种行为的目的而敲诈勒索；

(f) 本着实施第 1 条（1）（a）～（h）和第 2 条（2）（b）中所列举的某种行为的目的而草拟虚假的管理文件。

3．对如第 2 段中所描述的可处罚的行为，并不是一定指实际实施的恐怖行为。

[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.”

基于第 3 条，框架第 1（c）段，[863] 例如，当知道以下信息打算用于与恐怖活动有关的目的时，各成员国有责任对发布如何使用爆炸物的指南信息的行为予以判罪。需要找出这一信息的确打算用于与恐怖活动有关的目的的证据，很可能限制了法律条款的应用，原因是可以在国际互联网上找到大多数关于如何使用武器的指南信息，而它们的发布并不直接涉及恐怖攻击。由于大多数武器和爆炸物既可用于实施“普通”犯罪，也可用于实施恐怖活动（双重使用），因此，这一信息本身几乎不用能来证明发布它的人已经知道此类信息随后的用途。因此，需要考虑到信息发布的背景（例如，发布在由恐怖组织运营的某个网站上）。

5.2.2 经济合作与发展组织 [864]

1983 年，经济合作与发展组织（OECD）启动了一项研究，研究关于对各国刑法进行国际协调的可能性，以便解决计算机犯罪问题。[865] 1985 年，该组织发布了一份报告，分析了当前的法律，并提出了与网络犯罪作斗争的提议。[866] 经济合作与发展组织推荐了一份最小的犯罪行为清单，对这些犯罪行为，各国应考虑予以判罪，如与计算机有关的欺诈、与计算机有关的伪造、更改计算机程序和数据以及截获通信等。1990 年，信息、计算机和通信政策（ICCP）委员会组建了一个专家小组，以制定一系列有关信息安全的指导方针，这些指导方针到 1992 年起草完毕，之后 OECD 理事会批准了这些指导方针。[867] 这些指导方针在制裁问题上包括以下几方面内容：

> 在保护那些依靠信息系统的人的利益，使其免受因信息系统及其组成部分的可用性、机密性和完整性遭到攻击而造成的损害的过程中，对滥用信息系统的行为进行制裁是一种重要的手段。此类攻击的例子包括通过嵌入病毒和蠕虫、更改数据、非法访问数据、计算机欺诈或伪造以及未经授权的复制电脑程度等，来破坏或中断信息系统。在与此类危险行为作斗争的过程中，各国选择用多种方式来描述和响应这些攻击行为。国际上就这一问题日益达成共识，核心是：与计算机有关的违法行为应当纳入到国家刑法中来。在过去二十年间，这体现在了 OECD 各成员国在制定计算机犯罪和数据保护方面法律的工作中，也体现在了 OECD 和其他国际机构在制定与计算机相关犯罪作斗争的法律的工作中 [...[. 应定期评审国家法律，以确保它足以应对因滥用信息系统而带来的威胁。

1997 年，在对这些指导方针进行评审后，ICCP 于 2001 年设立了第二个专家小组来更新这些指导方针。2002 年，新版的指导方针《OECD 有关信息系统和网络安全的指导方针：着力培育安全文化》作为 OECD 理事会的一项建议书被采纳了。[868] 指导方针包含九条互补的原则：

---

[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.

[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

1）意识

参与者应意识到需要加强信息系统和网络的安全，并知道他们该如何加强信息系统和网络的安全。

2）责任

所有参与者都有责任保证信息系统和网络的安全。

3）响应

参与者应及时采取行动，并以合作的态度，来预防、侦查和响应安全事件。

4）道德

参与者应尊重他人的合法权益。

5）民主

信息系统和网络的安全应与民主社会的核心价值相一致。

6）风险评估

参与者应进行风险评估。

7）安全设计与实施

参与者应将安全视为信息系统和网络的一个不可或缺的重要要素。

8）安全管理

参与者应采用一种综合方法来实施安全管理。

9）再评估

参与者应对信息系统和网络的安全进行评审和再评估，并对安全政策、作法、措施和程序进行适当的修改。

2005 年，OECD 发表了一份报告，就垃圾邮件对发展中国家的影响进行了分析。[869] 报告指出，与西方国家相比，由于发展中国家的资源更有限、更昂贵，因此垃圾邮件的问题更加严重。[870]

在收到联合国秘书长行政办公室战略规划部门发出的请求后，请求制定一份有关国际互联网用于恐怖主义目的的各国国内法律解决方案比较纲要后，2007 年，OECD 发布了一份有关各国国内法律如何处置“网络恐怖主义”的报告。[871]

5.2.3 亚太经济合作组织 [872]

2002 年，亚太经济合作组织（APEC）领导人发表了“关于对抗恐怖主义和促进增长的宣言”，以制定全面的法律来应对网络犯罪，并提升国家的网络犯罪调查能力。[873] 这些国家致力于：

[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.
[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.

- 在 2003 年 10 月以前，制定一整套涉及网络安全和网络犯罪的综合法律，与国际法律手段的规定保持一致，包括联合国大会 55/63（2000）决议和《网络犯罪公约》（2001）；
- 在 2003 年 10 月以前，确定国家反网络犯罪部门和国际高科技援助联络点，并建设各国尚不具备的此类能力；
- 在 2003 年 10 月以前，设立一些机构来交流威胁信息和弱点评估结果（如计算机应急响应小组）。

APEC 领导人呼吁与网络犯罪作斗争的官员之间开展更加密切的合作。[874] 2005 年，APEC 组织召开了关于网络犯罪立法的会议。[875] 会议的主要目标是：

- 加快制定与网络犯罪作斗争、提升网络安全水平的综合法律框架；
- 协助执法机构应对迫在眉睫的问题以及因技术进步而带来的挑战；
- 促进区域间网络犯罪调查者之间的合作。

APEC 电信和信息工作小组 [876] 积极参与了 APEC 方法的制定，以增强网络安全水平。[877] 2002 年，它批准了 APEC 网络安全战略。[878] 通过参考联合国和欧洲理事会现有的国际方法，工作小组表述了他们在网络犯罪立法方面的立场。[879] 2008 年，在泰国曼谷举行的 APEC 电信和信息部长会议上发表了一份声明，声明强调了继续在与网络犯罪作斗争的过程中加强协调的重要性。[880]

5.2.4 英联邦

考虑到网络犯罪的日益重要性，英联邦的司法部长们决定命令一个专家小组来制定一个与网络犯罪作斗争的法律框架，它以《欧洲理事会关于网络犯罪的公约》为基础。[881] 这种方法旨在协调英联邦内的法律，以实现国际合作，原因是若不采取这种方法，那么在英联邦内就网络犯罪问题开展国际合作则需采用 1272 个双边条约。[882] 专家小组于 2002 年 3 月提交了他们的报告和建议。[883] 2002

[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: 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).

年底，《关于计算机和与计算机有关的犯罪的示范法》草案出台。[884] 由于专家小组提供了明确的指令，以及将《网络犯罪公约》视为一项国际标准，因此，这部示范法与《网络犯罪公约》中确定的标准是一致的。

5.2.5 阿拉伯联盟与海湾合作理事会 [885]

阿拉伯地区的许多国家已经采取了国家措施，并采用了一些方法来与网络犯罪作斗争，或者已经处于起草法律阶段。[886] 这些国家的例子包括：巴基斯坦、[887] 埃及[888] 和阿拉伯联合酋长国 [889]（UAE）。海湾合作理事会（GCC）[890] 在 2007 年的会议上建议该理事会的成员国寻求一种考虑到国际标准的共同方法。[891]

5.2.6 美洲国家组织 [892]

自 1999 年以来，美洲国家组织（OAS）一直在积极应对区域内的网络犯罪问题。其中，该组织在 REMJA 的管辖范围内举行了多次会议，REMJA 是美洲国家司法部长或部长或首席检察官的英文缩写。[893]

1999 年，REMJA 建议成立一个有关网络犯罪的政府间专家小组。委托专家小组从事以下工作：

- 对以计算机和信息为目标或者使用计算机作为犯罪手段的犯罪行为进行全面判断；
- 对涉及此类犯罪行为的国家法律、政策和做法进行全面判断；
- 确定一些具有相关专业技能的国家和国际实体；以及

---

[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.
4) Providing trainings to inspection and law enforcement officials on dealing with such crimes.
5) Providing sufficient number of experts highly qualified in new technologies and Cybercrime particularly in regard to proofs and collecting evidence.
6) 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.
7) 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.
8) 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.

[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.

- 确定在美洲国家间系统内进行合作的机制，以便与网络犯罪开展斗争。

2000 年，REMJA 提出了网络犯罪这一主题，并一致同意了许多建议。[894] 这些建议在 2003 年的会议上被再次提出，[895] 包括：

- 支持在首次会议上对政府专家小组提出的建议进行考虑，作为 REMJA 的文献，以便制定《美洲国家间与网络安全威胁作斗争战略》，它指的是 OAS 大会决议 AG/RES.1939（XXXIII-O/03），并要求专家小组通过主持会议，继续支持《战略》的准备工作。
- 各成员国在专家小组的背景下，对一些有助于各成员国之间在与网络犯罪作斗争和对网络犯罪作研究方面开展广泛和有效合作的机制进行了评审，可能的话，进一步提升技术和法律能力，以便加入由八国集团确立的 24/7 网络，从而为网络犯罪调查提供援助。
- 各成员国对实施《欧洲理事会关于网络犯罪的公约（2001 年）》各项原则的可取性进行了评估；并对加入该《公约》的可能性进行了考虑。
- 各成员国对国内负责执法的实体或机构的结构与工作进行了评审，并根据需要进行了更新，以适应网络犯罪特点的变化，其方法包括评审与网络犯罪作斗争的执法机构和提供传统警力支援或相互法律援助的机构之间的关系。

REMJA 第四次会议建议，在 OAS 工作小组的活动框架内接受 REMJA 的建议，重新召集应对网络犯罪的政府专家小组，[896] 并委托其从事以下工作：

- 继续实施由该工作小组提出的、并由 REMJA 第三次会议采纳的建议；以及
- 考虑准备有关的美洲国家间法律手段和示范法，以便加强在与网络犯罪作斗争过程中的协调合作，考虑与隐私、信息保护、程序问题和预防犯罪等方面有关的标准。

迄今为止，REMJA 已经举行了七次会议。[897] 最近的两次会议是 2006 年 4 月和 2008 年 4 月在美国华盛顿特区举行的。2006 年会议提出的建议包括以下内容：[898]

- 继续加强与欧洲理事会的合作，以使 OAS 各成员国可以考虑运用《欧洲理事会关于网络犯罪的公约》中的各项原则[899]，支持这种努力，并采纳实施这些原则所需的法律措施和其他措施。同样地，继续努力强化与网络犯罪领域中其他国际组织和机构之间互换信息与开展合作的机制，如联合国（UN）、欧盟（EU）、亚太经济合作组织（APEC）、经济合作与发展组织（OECD）、八国集团（G8）、英联邦、国际刑警组织（INTERPOL）等，以便 OAS 各成员国能够利用这些组织和机构在与网络犯罪作斗争过程中所取得的成果和进展；以及
- 各成员国设立负责调查网络犯罪的专门部门，确定在这一问题上充当联络点、负责促进信息互换和证据获取的主管部门。此外，要在政府主管部门、国际互联网服务提供商和提供数据传输服务的其他私营部门之间，推动与网络犯罪作斗争有关的合作。

---

[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.

[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

在 2008 年的会议上重申了这些建议，会议进一步指出：[900]

- 牢记政府专家小组和上一次 REMJA 会议采纳的建议，各国应考虑运用《欧洲理事会关于网络犯罪的公约》中的各项原则，同意这些原则，并采纳实施这些原则所需的法律措施和其他措施。同样地，出于这一目的，在 OAS 总秘书处的赞助下，通过法律事务秘书处和欧洲理事会，仍需继续开展技术合作活动。同样地，仍需继续努力加强与网络犯罪领域中其他国际组织和机构的信息交流与合作，以便 OAS 各成员国能够利用这些组织和机构在与网络犯罪作斗争过程中所取得的成果和进展；
- 美洲国家间反恐委员会（CICTE）秘书处、美洲国家间电信委员会（CITEL）以及网络犯罪工作小组，将继续推动永久的协调和合作活动，以确保通过 OAS 大会决议 AG/RES. 2004（XXXIV-O/04）所采纳的《美洲国家间全面网络安全战略》的实施。

5.3 科学方法

为在全球层面应对网络犯罪问题而制定一个法律框架，一种广为人知的科学方法是《斯坦福国际公约》草案（CISAC）。[901] 该《公约》是在 1999 年美国斯坦福大学举行的一次会议后制定的。[902] 与《欧洲理事会关于网络犯罪的公约》[903] 相比，大约在同一时间起草的《斯坦福国际公约》草案显示了许多相似之处。二者都涵盖了实体刑法、程序法以及国际合作等方面的问题。最重要的区别在于以下事实：《斯坦福公约》草案中提到的违法行为和程序手段，只有在信息基础设施遭到攻击和恐怖攻击时才适用，而《欧洲理事会关于网络犯罪的公约》中提到的、与程序法和国际合作有关的手段，还适用于传统的犯罪行为。[904]

5.4 不同国际与法律方法之间的关系

在技术协议方面单一标准的成功施行提出了一个问题，那就是：如何避免不同国际方法之间的冲突。[905] 当前的《网络犯罪公约》是一种恰当的主要国际框架，涵盖了网络犯罪所有的相关方面，

---

[900] Conclusions and Recommendations of REMJA-VII, 2008, available at: http://www.oas.org/juridico/english/cybVII_CR.pdf

[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.

但其他一些倡议也在讨论中。第二种国际方法是当前正由国际电联采取的方法。[906] 在信息社会世界峰会之后，国际电联被认为是所谓的信息社会世界峰会行动线 C5 的推动者。如在 2003 年信息社会世界峰会日内瓦阶段会议所定义的那样，行动线 C5 包含在使用信息通信技术中树立信心和提升安全等内容。[907] 在有关行动线 C5 后续行动的第二次促进会议上，国际电联秘书长强调了在与网络犯罪作斗争过程中国际合作的重要性。随后，国际电联宣布制定《全球网络安全议程》。[908] 国际电联《全球网络安全议程》（GCA）包含七大目标。[909] 其中之一是详细制定针对网络犯罪示范法立法的战略。为制定与 GCA 有关的战略，国际电联成立了一个专家小组。[910] 一部可能的示范法如何与现有的标准相辅相成？这一问题的答案取决于在起草一部新的示范法时所采用的方法。一般地，存在三种可能的关系：

- 有争议的管制

  如果一部新的示范法定义了不符合现有标准的标准，那么这至少在一开始可能会对必要的协调过程产生负面影响。

- 部分复制《公约》中的标准

  一部新的示范法可以基于《网络犯罪公约》，并可以不包含那些导致《公约》难以得到签署，甚至阻止某些国家签署《公约》的规定。一个例子是在《网络犯罪公约》第 32b 条中曾倍受争议的规定。该规定在 2007 年的网络犯罪委员会会议上遭到了俄罗斯代表团的批评。[911]

- 增补《公约》中的标准

  一部新的示范法可以超出《网络犯罪公约》中所定义的标准，例如，对某些与网络犯罪有关的行为进行判罪，以及定义一些《公约》中尚未涵盖的程序手段。自 2001 年起，形势已经发生了许多重大变化。在起草《公约》时，“网络钓鱼”、[912] “身份盗用”[913] 以及与在线游戏和

---

[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.

[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:

社会网络有关的违法行为，也不像它们之前那样关系重大。一部新的示范法可以通过纳入更多的、具有跨国影响的违法犯罪行为来继续其法律协调过程。[914]

在这方面，国际电联针对网络犯罪法律的工具组[915]着眼于为各国提供参考材料，帮助它们制定法律框架，以阻止网络犯罪。它强调了各国对其法律框架进行协调的重要性，以便更有效地与网络犯罪作斗争，并促进国际合作。国际电联针对网络犯罪法律的工具组，是由一个各学科的国际专家小组提出的，并在2009年初推出了其第一个草案。

5.5 国际与国家法律方法之间的关系

正如此前所指出的那样，网络犯罪是一种真正的跨国犯罪。[916]一般地，攻击者可以瞄准世界任何国家的用户进行打击，基于这一事实，执法机构之间开展国际合作是对国际网络犯罪进行调查的一项基本要求。[917]调查需要合作手段，并有赖法律协调。由于双重犯罪这一公共原则，[918]有效的合作首先要求对实体刑法规定进行协调，以防止出现“安全避风港”。[919]此外，需要协调调查手段，以确保国际调查涉及的所有相关国家都具有所需的调查手段，以便完成调查工作。最后，执法机构之间的有效合作要求采用与实际问题有关的有效程序。[920]因此，协调联动机制的重要性以及在全球协调过程中联合参与的需求，对任何国家的反网络犯罪战略而言，即使不是一种必然，至少也是一种趋势。

5.5.1 国家方法得以普及的原因

尽管国际社会广泛认可协调的重要性，但执行国际法律标准的过程远未完善。[921]为什么国家方法在与网络犯罪作斗争的过程中起着重要作用？其中一个原因是犯罪活动的影响并非普遍相同。国家方法的一个例子是在反垃圾邮件斗争中所采取的方法。[922]涉嫌垃圾邮件的电子邮件对发展中国家的影响尤其严重，对该问题，在经济合作与发展组织（OECD）的一份报告中进行了分析。[923]由于

---

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 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.

发展中国家的资源更稀少、更昂贵，因此与西方国家相比，垃圾邮件对发展中国家的影响要严重得多。[924] 网络犯罪的影响不同，加上现有法律结构和惯例的差别，是众多国家层面的法律措施不执行或者只是部分执行国际标准的主要原因。

5.5.2 国际解决方案对国家解决方案

在技术全球化的时代，这种讨论看起来有点奇怪，原因是任何希望连接国际互联网的人都需要利用一些适当的（技术）标准协议。[925] 单一的标准是网络运营的一项基本要求。不过，不像技术标准，法律标准仍存在差异。[926] 在网络犯罪国际化的趋势下，它必须回答国家方法是否依然适用这个问题。[927] 这一问题与用于执行不符合现有国际标准的法律的所有国家和区域方法都相关。缺乏协调可严重阻碍国际调查，而那些国际标准之外的国家和区域方法，可在实施国际调查中避免问题和困难。[928]

区域和国家方法日渐增多，有两个主要原因。首先是立法速度。欧洲理事会既不强迫任何成员国签署《网络犯罪公约》，也不强迫《公约》签署国批准它。因此，与国家和区域法律方法相比，协调过程常常看起来比较慢。[929] 与欧洲理事会不同，欧盟采取了一些方法来强迫各成员国执行框架决定和指令。这就是为什么 2001 年签署了《网络犯罪公约》但尚未批准它的许多欧盟成员国仍执行 2005 年欧盟关于信息系统攻击的框架决定的主要原因。

第二个原因与国家和区域差异有关。有些违法行为只在区域中的某些国家才会被定罪。这方面的例子是宗教违法行为。[930] 尽管要对有关涉嫌侮辱宗教符号的违法行为的刑法条款进行国际协调看起来是不可能的，但在这方面，国家方法可以确保某国的法律标准得以维持。

5.5.3 国家方法的困难

国家方法面临许多问题。至于传统犯罪，一个或几个国家对某些行为的判罪，可以严重影响违法者在这些国家进行违法活动的能力。不过，当涉及与国际互联网有关的违法行为时，单个国家对违法者的影响力将大打折扣，原因是，在通常情况下，只要连接到国际互联网，违法者就可以从世界任何地方进行其违法活动。[931] 如果他们从并不对这些行为判罪的某个国家实施违法行为，那么国际调查以及引渡请求常常会失败。因此，国际法律方法的关键目标之一是通过规定和采用全球标准，防止出现对违法者而言是安全的“避风港”。[932] 因此，一般地，国家方法需要采用额外的辅助措施，使之能够发挥作用。[933] 最常见的辅助措施是：

---

[924] See Spam Issue in Developing Countries, Page 4, available at: http://www.oecd.org/dataoecd/5/47/34935342.pdf.
[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.

- 除了对非法内容的提供商判罪以外，还对其使用者进行判罪

  一种方法是除了对提供非法服务单独判罪之外，还对其使用非法服务进行判罪。对管辖范围内的使用者进行判罪是对在国外实施违法行为的服务提供商无法进行判罪的一种补偿方法。

- 对在犯罪实施过程中使用的服务进行判罪

  第二种方法是管制，甚至在管辖范围内对某些用于犯罪目的的服务进行判罪。这一解决方案胜于第一种方法，原因是它牵涉提供中性服务的企业和组织，这些中性服务既可用于合法行为，也可用于非法行为。这种方法的一个例子是美国于 2006 年制定的《非法国际互联网赌博强制法案》。[934]

与这一措施密切相关的是，确定对国际互联网上可用的某些内容进行过滤的义务。[935] 在著名的雅虎（Yahoo）决定中，[936] 就曾讨论过这一方法，而且这一方法目前正在以色列展开讨论，该国的接入提供商有义务限制访问某些含有成人内容的网站。对国际互联网内容实施控制的尝试不仅仅限于成人内容；一些国家还利用过滤技术来限制对涉及政治主题的网站的访问。开放网络倡议[937] 报告说，大约有二十四个国家实施了这种审查制度。[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. 法律响应

本章通过解释对某些行为进行定罪的法律方法，来概述对网络犯罪现象的法律响应。[939] 只要是有可能运用国际方法的案例，就采用国际方法。而对无法采用国际方法的案例中，将提供国家或区域方法的例子。

6.1 实体刑法

6.1.1 非法访问（黑客行为）

由于计算机网络的发展、它们能够连接其他计算机并且能够为用户提供对其他计算机系统的访问，因此计算机已被黑客们用于犯罪目的。[940] 黑客的动机已出现实质性变化。[941] 黑客不必出现在犯罪现场；[942] 他们只需绕过网络的安全保护措施就行。[943] 在许多非法访问的案例中，即使是在同一幢建筑物内，保护网络硬件物理设施的安全系统也比保护网络上敏感信息的安全系统更为先进。[944]

非法访问计算机系统使计算机操作者无法以一种不受干扰和不受约束的方式来管理、操作和控制其系统。[945] 保护的目的是维护计算机系统的完整性。[946] 至关重要的是区分非法访问和后续的违法行为（如数据刺探 [947]），原因是法律条款对保护的着重点不同。在大多数情况下，非法访问（在这些情况下，法律着重于保护计算机系统本身的完整性）并非最终目标，而只是进一步犯罪的第一步，比如修改或获取储存的数据（在这些情况下，法律着重于保护数据的完整性和机密性）。[948]

问题是：除了对后续的违法行为应当予以定罪之外，对其第一步，即非法访问行为是否应当也予以定罪？[949] 在国家层面对各种各样对非法访问计算机进行定罪的方法分析表明，一些已制定的规定有时候将非法访问与后续的违法行为混为一谈了，或者着眼于仅对造成严重侵犯的非法访问给予定罪。[950] 有些国家对单纯的非法访问也进行定罪，而另一些国家则只对以下行为予以定罪，即被访

---

[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/Lotrionte*, 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.

问系统受到安全措施的保护、或者作案者具有恶意、或者数据已被作案者获取、修改或破坏。[951] 还有一些国家不对非法访问本身定罪，而只对后续的违法行为定罪。[952] 反对对非法访问本身定罪涉及以下情形，即单纯的侵入并未造成任何危险，或者“黑客”行为反而使目标计算机系统察觉到了安全漏洞和弱点。[953]

《网络犯罪公约》：

《网络犯罪公约》包括一个关于非法访问的条款，该条款通过对未授权的系统访问进行定罪，来保护计算机系统的完整性。注意到国家层面上方法的不一致，[954]《公约》提供了限制的可能性 — 至少在大多数情况下是这样 — 使得一些没有针对非法访问进行立法的国家能够对这一问题保留更为宽松的法律。[955]

条款：

> **第 2 条 — 非法访问**
>
> 当针对整个计算机系统或其任何部分的访问是未经授权而故意进行时，各方应采取依据本国法律认定犯罪行为所需的法律手段和其他手段。签约方可以规定违法行为应具有获得计算机数据的意图或其他不诚实的意图，或者涉及与另一个计算机系统相连接的计算机系统，而侵害其安全措施。

包括的违法行为：

“访问”这一术语并没有规定一种特定的通信手段，而是可扩展的，并且对进一步的技术发展是开放的。[956] 它应包括可用于进入另一个计算机系统的所有手段，包括国际互联网攻击，[957] 以及非法访问无线网络。甚至法律条款还涵盖对没有连接到任何网络的计算机的访问（例如，通过绕过密码保护措施）。[958] 这种广义的方法意味着非法访问不仅包括未来的技术发展，而且也包括内部人员

---

[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.

[958] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

和员工对秘密数据的访问。[959] 第 2 条第二句提供了限制对经由网络的非法访问进行定罪的可能性。[960]

因此，以一种对未来发展保持开放的方式定义了非法行为和受保护的系统。《解释报告》将硬件、组件、储存的数据、目录、通信流量以及与内容有关的数据列为可被访问之计算机系统组成部分的例子。[961]

心理因素：

与《网络犯罪公约》定义的所有其他违法行为一样，第 2 条要求违法者是有意实施了违法行为。[962]《公约》并没有包含对“有意”这一术语的定义。在《解释报告》中起草者指出，“有意”应当在国家层面上进行定义。[963]

未获授权：

根据《公约》第 2 条，只有当访问是“未获授权”时，对计算机的访问才可被起诉。[964] 对允许公众自由和公开访问的系统进行访问，或者获得了系统拥有者或其他权利持有者授权的访问，则不属于“未获授权”。[965] 除了自由访问这一主题，还应解决安全测试程序的合法性问题。[966] 网络管理员以及为确定安全措施上可能的缺陷而对计算机系统保护措施进行测试的安全公司，都对根据非法访问而定罪的可能性保持警惕。[967] 尽管这些专业人士通常获得拥有者的许可而操作，并因此是合法开展工作的，但《公约》的起草者强调，“获得拥有者或操作者授权而对计算机系统安全性进行测试或保护，[...]视为获得授权”。[968]

当犯罪的受害者向违法者交出密码或类似的访问代码时，并不一定意味着违法者访问受害者的计算机系统时是经授权的访问。如果通过一种成功的社会工程方法，[969] 违法者说服受害者透露密码

---

[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).

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

或访问代码，那么有必要验证受害者提供的授权是否涵盖违法者所实施的行为。[970] 一般地，情况并非如此，因此违法者的行为是未获授权的。

限制与保留：

作为一种可替代的广义方法，《公约》提供了用额外因素来限制定罪的可能性，这列举在第二句话中。[971] 《公约》的第 42 条规定了如何使用这一保留的程序。[972] 可能的保留涉及安全措施、[973] 获取计算机数据的特殊意图、[974] 其他为犯罪过失辩护的不诚实意图，或者要求通过网络对计算机系统实施违法行为。[975] 在欧盟[976] 《关于针对信息系统攻击的框架决定》[977] 中可以找到一种类似的方法。

《英联邦计算机以及与计算机有关的犯罪的示范法》：

在 2002 年版的《英联邦示范法》的第 5 节中可以找到一种类似的方法。[978]

> **第 5 节**
>
> 有意、没有合法或正当理由访问整个计算机系统或其局部的人，即在实施可处罚的违法行为，在定罪时，处以不超过[一定期限]的监禁，或者不超过[一定数量]的罚款，或者两项并罚。

《网络犯罪公约》与《英联邦示范法》的主要区别在以下事实，即不同于《网络犯罪公约》第 2 条，《英联邦示范法》第 5 节未包含可保留的选择方案。

---

[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.

《斯坦福公约》草案：

非正式的[979] 1999 年版的《斯坦福公约》草案将非法访问视为签字国应当予以定罪的违法行为之一。

条款：

> **第 3 条 — 违法行为**
>
> 1. 根据这一《公约》，如果任何人在未获得法律认可的授权、许可或同意的前提下非法且有意地从事以下任何行为，那么认为就是在实施违法行为：
>
> [...]
>
> （c）以明显的、明确的方式进入一个限制访问的网络系统；
>
> [...]

包括的违法行为：

草案条款与《网络犯罪公约》第 2 条有许多相似之处。两者都要求是未获权利/未获授权而实施的有意行为。在这一背景下，草案条款的要求（“未获得法律认可的授权、许可或同意”）比《网络犯罪公约》中使用的“未获授权”[980] 这一术语更加精确，而且明确着眼于融入自我防卫的概念。[981] 与《公约》的主要差别在于，草案条款使用了“网络系统”这一术语。网络系统在《公约》草案的第 1 条第 3 段中定义。它涵盖用于转发、传输、协调或控制数据或程序通信的任何计算机或计算机网络。该定义与《网络犯罪公约》第 1 条 a）中提供的“计算机系统”这一术语有许多相似之处。[982] 尽管《公约》草案指的是与数据交换有关的行为，并因此主要着重于基于网络的计算机系统，但两个定义都包括了互联的计算机以及单机。[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 数据刺探

《网络犯罪公约》、《英联邦示范法》以及《斯坦福公约》草案，都只为非法截获提供了法律解决方案。[984] 存在疑问的是，《网络犯罪公约》的第 3 条是否适用于通过截获数据传输过程实施的违法行为以外的其他案件。如以下所说明的那样，[985] 《公约》是否涵盖对存储在硬盘上的信息进行的非法访问，这个问题得到了激烈讨论。[986] 由于必须是数据传输过程，因此有可能《网络犯罪公约》第 3 条并不涵盖截获传输过程以外的数据刺探行为。[987]

在这一背景下，一个经常被讨论的问题是，是否对非法访问的定罪使得对数据刺探的定罪变得没有必要。在违法者可以合法访问计算机系统的情形中（比如，由于他被命令修复计算机），而且在这一场合（违反了有限的合法权限）从系统中拷贝了文件，这一行为通常没有包括在对非法访问定罪的条款中。[988]

鉴于当代许多至关重要的数据都保存在计算机系统中，因此有必要评估现有的数据保护机制是否恰当，或者是否其他刑法条款是保护用户免遭数据刺探的必要法律措施。[989] 如今，计算机用户可以使用各种各样的硬件设备和软件工具来保护秘密信息。他们可以安装防火墙、访问控制系统或者对保存的信息进行加密，并且通过这种方法来降低数据刺探的风险。[990] 尽管用户友好的设备可供使用，而且对使用者的知识要求不高，但对计算机系统上数据的真正有效保护，通常要求用户具有一定知识，而这些知识是大多数用户所不具备的。[991] 特别是保存在私人计算机系统上的数据，通常并没有得到恰当的保护以防遭到数据刺探。因此，刑法条款可以提供额外的保护。

示例：

有些国家已决定通过对数据刺探定罪，借助技术措施来延伸这种可用的保护。主要方法有两种。有些国家采用一种狭义方法，只有当特定的秘密数据被违法者获取时，才对数据刺探定罪 — 例如 18 U.S.C § 1831，该条款对经济刺探进行定罪。条款不仅没有涵盖数据刺探，而且也没有涵盖获取秘密信息的其他手段。

---

[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.

§ 1831.经济刺探

（a）一般地 — 无论何人，打算或知道违法行为将使任何外国政府、外国执行部门或者外国机构受益，有意地 —

（1）窃取，或者未经授权而盗用、获取、带走、隐藏或者通过欺诈、诡计或骗术，获取商业秘密；

（2）未经授权拷贝、复印、勾勒、画出、拍摄、下载、上载、更改、破坏、影印、复制、传输、发送、邮寄、交流或带走商业秘密；

（3）接受、购买或占有商业秘密，明知同一件商业秘密是窃取或盗用、未经授权而获取或转换的；

（4）试图实施第（1）段至第（3）段中任何一段所述的违法行为；或者

（5）与一人或多人密谋实施第（1）段至第（3）段中任何一段所述的违法行为，而这些人中的一人或多人实施了达到密谋目标的任何行为；

除了（b）小节中所述的情形，须处以不超过 50 万美元的罚款或者不超过 15 年的监禁，或者两项并罚。

（b）组织 — 对任何实施（a）小节中所述之违法行为的组织，须处以不超过 1000 万美元的罚款。

另一些国家采用一种更为广义的方法，并且对获取已储存之计算机数据的行为予以定罪，即使这些数据没有包含经济秘密。一个例子是旧版本的德国刑法§ 202a。[992]

第 202a 节 数据刺探：

（1）对任何未经授权的个人，为自己或他人获取并不属于他、且对未授权访问采取了特别保护措施的数据，应处以不超过三年的监禁或者处以罚款。

（2）第 1 小节中所指的数据，仅仅指以电子方式或磁力方式或者任何非直接可视形式而保存或发送的数据。

该条款不仅涵盖经济秘密，而且一般涵盖存储的计算机数据。[993] 从实现保护这一目标角度来看，这种方法比§ 1831 USC 更加广泛，但是该条款的应用是有限的，原因是只有当数据受到防止未授权访问的特别保护时才会对获取数据这种行为进行定罪。[994] 因此，根据德国刑法，对保存的计算机数据的保护，仅限于已采取措施避免成为此类违法行为受害者的个人或企业。[995]

该条款的相关性：

该条款的执行尤其与以下案件相关，即违法者获得授权访问计算机系统（比如，由于他接到命令修复计算机），然后滥用了这一授权，非法地获取了计算机系统上所保存的信息。[996] 至于授权涵盖对计算机系统的访问这一事实，一般不可能用对非法访问定罪的条款来涵盖。

[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.
[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; *Tadro*s, Stolen photos from laptop tell a tawdry tale,

未获授权：

数据刺探条款的运用一般要求数据是在未获得受害者同意的情况下获取的。成功的网络钓鱼攻击[997]清楚地表明，骗局的得逞基于对用户的操纵。[998]由于获得了受害者的同意，成功操纵用户透露秘密信息的违法者，无法根据上述条款来起诉。

6.1.3 非法截获

信息通信技术的使用伴随着一些与信息传输安全有关的风险。[999]与一国中传统的邮购业务不同，通过国际互联网的数据传输过程涉及多个提供商以及数据传输过程可能被截获的不同点。[1000]对于截获，最大的弱点依然是用户，尤其是那些私人家庭计算机的用户，他们通常没有针对外部攻击采取适当的保护措施。由于违法者一般总是瞄准最大弱点，因此针对私人用户的攻击风险是很大的，如果是以下情形，则风险更大：

- 易受攻击技术的发展；以及
- 对违法者而言个人信息日益增大的相关性。

新的网络技术（如“无线局域网”）为国际互联网访问提供了若干优势。[1001]例如，在私人家庭里建立一个无线网络，使家人能够在一定半径之内的任何地方连接至国际互联网，而无需采用电缆连接方式。但这一技术的大行其道以及它所带来的便捷，也伴随着一些涉及网络安全的严重风险。如果作案者可以使用一个未受保护的无线网络，那么他可以登录到这一网络，并用它来实施犯罪活动，而无需进入这户人家的建筑物。作案者只要走到无线网络的半径之内便可实施攻击。现场测试结果表明，在有些地区，多达 50%的私人无线网络都没有针对未授权截获或访问采取保护措施。[1002]在大多数情况下，缺乏保护是源于缺乏如何配置保护措施的知识。[1003]

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.

[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.

过去，非法截获的作案者重点以商业网络为作案对象。[1004] 比起截获在私人网络中传输的数据，截获公司的通信更有可能获取有用的信息。然而，针对个人数据的身份盗用案件数量的日益增多，意味着作案者的作案对象已经发生了改变。[1005] 诸如信用卡号码、社会保险号、[1006] 密码以及银行账号信息等私人数据，如今越来越引起违法者的兴趣。[1007]

《网络犯罪公约》：

《网络犯罪公约》包含一条保护非公开传输完整性的条款，方法是对其未授权截获行为进行定罪。这一条款旨在等同于通过保护语音交谈内容不被非法窃听和/或非法录音的方法，来对电子传输进行保护，当前，这一条款在大多数法律体系中已经存在。[1008]

条款：

> **第 3 条 — 非法截获**
>
> 当从计算机系统或在计算机系统内，通过技术手段，对非公共传输之计算机数据的截获是未经授权而故意进行时，包括来自携带此类计算机数据的计算机系统中的电磁辐射，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为。签约方可以要求所犯罪行应具有不诚实意图，或者与连接至另一个计算机系统的某个计算机系统有关。

包括的违法行为：

第 3 条的适用性限于借助技术手段实施的、对传输的截获。[1009] 与电子数据有关的截获可以定义为在传输过程期间获取数据的任何行为。[1010]

如上所述，对条款是否涵盖对储存在硬盘上的信息的非法访问这一问题进行了有争议的讨论。[1011] 一般地，该条款只适用于对传输的截获 — 访问已储存的信息不被认为是对传输的截获。[1012]

[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 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.

事实是，即使在违法者物理接入一个独立计算机系统的情况下，对该条款的应用也要进行讨论，部分是由于以下事实，即《网络犯罪公约》没有包含与数据刺探[1013]有关的条款，而且《公约》的《解释报告》包含两条针对第 3 条应用情况的、稍显不严密的解释：

- 《解释报告》首先指出，条款涵盖了发生在计算机系统内的通信过程。[1014] 不过，这依然留下一个未解决的问题，即条款是只应适用于受害者发送数据且随后被违法者截获的情形，还是也应适用于违法者本人操作计算机的情形。
- 指导方针指出，截获或者可以通过使用窃听设施来间接实施，或者可以“通过访问和使用计算机系统”[1015] 来实施。如果违法者访问计算机系统，并在未获授权的情况下用它来拷贝储存于外部磁盘驱动器上的数据，而这种行为导致了数据传输（从内部硬盘向外部硬盘发送数据），那么认为这一过程不是由违法者*截获的*，而是由违法者*发起的*。有关技术截获缺失的要素是，反对条款用于非法访问储存信息案件的强有力论据。[1016]

“传输”这一术语涵盖所有的数据传输，不论是通过电话、传真、电子邮件，还是通过文件进行的传输。[1017] 根据第 3 条确定的违法行为仅适用于非公共的传输。[1018] 如果传输过程是机密的，那么传输就是“非公共的”。[1019] 区分公共的传输和非公共的传输，至关重要的因素不是所传输数据的特性，而是传输过程本身的特性。甚至是传输公共可用的信息，如果涉及传输的各方意在使内容成为其通信秘密，那么也可被视为犯罪。使用公共网络不排除“非公共的”通信。

心理因素：

与《网络犯罪公约》定义的所有其他违法行为一样，第 3 条要求违法者是有意地实施了违法行为。[1020]《公约》不包含对“有意地”这一术语的定义。在《解释报告》中，起草者指出，对“有意地”这一术语应在国家层面上进行定义。[1021]

未获授权：

根据《公约》第 3 条，只有当访问是“未获授权”时，对通信的截获才可被起诉。[1022]《公约》的起草者提供了一组不属于“未获授权”截获的例子：

[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.

[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’*

- 基于传输各参与者指令或者授权的活动；[1023]
- 各参与者一致同意的授权测试或保护活动；[1024]
- 基于刑法规定或者出于国家安全的利益而实施的合法截获。[1025]

另一个在《公约》谈判过程中出现的问题是，信息记录程序的使用是否会导致基于第 3 条的刑事制裁。[1026] 起草者指出，通用的商业惯例（如信息记录程序）不被视为未获授权的截获。[1027]

限制与保留：

通过要求列举在第二句中的额外要素，包括“不诚实的意图”或者涉及连接至另一个计算机系统的计算机系统，第 3 条为限制定罪提供了选择方案。

《英联邦计算机以及与计算机有关的犯罪的示范法》：

在 2002 年版的《英联邦示范法》的第 8 节中可以找到一种类似的方法。[1028]

> **第 8 节**
>
> 任何人借助技术手段而有意地、没有合法或正当理由地：
>
> (a) 从计算机系统或在其内部截获任何非公共的传输；或者
>
> (b) 截获带有计算数据的、来自计算机系统的电磁辐射；即在实施可处罚的违法行为，在定罪时，处以不超过[一定期限]的监禁，或者不超过[一定数量]的罚款，或者两项并罚。

《斯坦福公约》草案：

非正式的 [1029] 1999 年版的《斯坦福公约》草案没有明确地对截获计算机数据的行为进行定罪。

---

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.

[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

6.1.4 数据干扰

对有形的或者物理的物体进行保护，防止它们受到有意破坏，是国家刑法的一个传统要素。随着数字化进程的继续，更多重要的企业信息作为数据存储起来。[1030] 对这种信息进行攻击或者获取它们，可导致经济损失。[1031] 除了删除它们，对此类信息的更改也会造成严重后果。[1032] 过去的法律没有按照对有形物体的保护那样，对数据进行如此彻底的保护。这使得违法者能够设计一些不至于招致刑事制裁的骗局。[1033]

《网络犯罪公约》：

在第 4 条中，《网络犯罪公约》包括了一条用于保护数据免受未经授权干扰的条款，以维护数据的完整性。[1034] 该条款的目的是填补某些国家刑法的现有不足，并且为计算机数据和计算机程序提供类似于有形物体保护的保护措施，使之免受有意破坏。[1035]

条款：

> **第 4 条 — 数据干扰**
>
> (1) 当对计算机数据的毁坏、删除、破坏、更改或限制是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为。
>
> (2) 签约方可以保留权利，要求将第 1 段中所述的、导致严重伤害的行为判定为犯罪行为。

包括的违法行为：

- “毁坏”和“破坏”这两个术语指的是对数据和程序之信息内容的完整性造成不利改变的任何行为；[1036]

---

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.

[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.

- “删除”涵盖将信息从存储介质中移去的各种行为，并将其视为与销毁有形物体的行为相当。尽管《公约》起草者提供了定义，但并没有区分删除数据的各种不同方法。[1037] 将文件丢入虚拟的垃圾箱并没有从硬盘中移去该文件。[1038] 甚至“清空”垃圾箱也不一定就移除了该文件。[1039] 因此，目前尚不确定，已被删除文件的恢复使用是否有碍该条款的应用。[1040]
- “限制”计算机数据指的是影响可访问介质之人的数据可用性的行为，在这一行为下，信息以一种不利的方式予以保存。[1041] 就拒绝服务 [1042] 攻击，对这一条款的应用特别地进行了讨论。[1043] 在这种攻击期间，在攻击目标的计算机系统上提供的数据，潜在用户以及计算机系统的拥有者已经无法再用。[1044]
- “更改”这一术语涵盖对现有数据所做的修改，不一定降低数据的可用性。[1045] 这种行为尤其涵盖在受害者的计算机上安装恶意软件等行为，如刺探程序、病毒或广告恶意软件等。[1046]

心理因素：

与《网络犯罪公约》所定义的所有其他违法行为一样，第 4 条要求违法者有意实施了违法行为。[1047] 《公约》没有包含对“有意”这一术语的定义。在《解释报告》中，起草者指出，对“有意”应在国家层面上进行定义。[1048]

[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.

[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.

未获授权：

与以上讨论的条款一样，这一行为必须是“未获授权”而实施的。[1049] 此前已经讨论过更改数据的权力，尤其是在“重发邮件器”的背景下。[1050] 重发邮件器用于修改某些数据，目的是方便匿名通信。[1051]《解释报告》指出，原则上，这些行为被认为是对隐私的一种合法保护，因此，可被视为是获得过授权的行为。[1052]

限制与保留：

通过将其限于造成了严重损害的案件，第 4 条提供了限制定罪的选择方案，这是一种类似于欧盟关于信息系统攻击的框架决定的方法，[1053] 它使各成员国能够限制针对“不是未成年人案件”的实体刑法条款的适用性。[1054]

《英联邦计算机以及与计算机有关的犯罪的示范法》：

在 2002 年版的《英联邦示范法》第 8 节中可以找到一种与《网络犯罪公约》第 4 条相一致的方法。[1055]

> **第 6 节**
>
> （1）无论何人，没有合法或正当的理由，有意或鲁莽地实施了下列任何一种行为：
>
> （a）破坏或更改数据；或者
>
> （b）使数据变得无意义、无用或无效；或者
>
> （c）阻碍、中断或干扰对数据的合法使用；或者

[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.

（d）阻碍、中断或干扰正在合法使用数据的人；或者

（e）拒绝任何有权访问的人访问数据；

即在实施一种可处罚的违法行为，在定罪时，处以不超过[一定期限]的监禁，或者不超过[一定数量]的罚款，或者两项并罚。

（2）无论人们的行为是具有临时效应还是具有永久效应，第（1）小节都适用。

《斯坦福公约》草案：

非正式的[1056] 1999 年版的《斯坦福公约》草案包含两条对与干扰计算机数据有关的行为进行定罪的条款。

条款：

第 3 条

1. 根据这一《公约》，如果任何人在未获得法律认可的授权、许可或同意的情况下非法且有意地从事以下任何行为，即认为是在实施违法行为：

（a）本着以下目的，即导致或明知此类行为将导致上述网络系统或另一个网络系统如其所预期的那样停止运转，或者不按该网络系统拥有者所预期的那样运行，来创建、存储、更改、删除、传输、转移、误传、操纵或干扰网络系统中的数据或程序，根据本《公约》，将被视为非法行为；

（b）出于以下目的以及为了产生相应的不良效应，即提供错误信息，以便对个人或财产造成实质性损坏，来创建、存储、更改、删除、传输、转移、误传、操纵或干扰网络系统中的数据或程序；

包括的违法行为：

《网络犯罪公约》、《英联邦示范法》与《公约》草案之间的主要区别在以下事实，即《公约》草案仅对干扰了计算机系统运转的干扰数据行为（第 3 条第 1a 段）进行定罪，或者当所实施行为的目的是提供错误信息以便对个人或财产造成损坏时（第 3 条第 1b 段），对之进行定罪。因此，草案法没有对删除数据存储设备中普通文本文件的行为进行定罪，原因是这一行为既不会影响计算机的运转，也不会提供错误信息。通过保护计算机数据的完整性，且不带进一步效应的强制性要求，《网络犯罪公约》和《英联邦示范法》都遵循了一种更广义的方法。

[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 系统干扰

提供基于信息通信技术服务的个人或企业，依赖其计算机系统的正常运转。[1057] 拒绝服务（DOS）攻击[1058] 使受害者的网页无法使用，展示了这种攻击的威胁有多么严重。[1059] 此类攻击可以造成巨大的经济损失，并甚至影响到更强大的系统。[1060] 企业并非是唯一目标。全世界的专家目前正在讨论一些可能出现的“网络恐怖主义”情形，尤其重视对关键基础设施的攻击，如供电系统和电信服务系统等。[1061]

《网络犯罪公约》：

为了保护运营商和用户对信息通信技术的使用，《网络犯罪公约》在第 5 条中包括了一条对有意干扰合法使用计算机系统的行为进行定罪的条款。[1062]

条款：

> **第 5 条 — 系统干扰**
>
> 对于通过输入、传输、破坏、删除、毁坏、更改或限制计算机数据，有意地、未经授权地严重阻碍计算机系统运转的行为，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为。

[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/Ronfeld*t, 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.

包括的违法行为：

这一条款的应用要求干扰了计算机系统的正常运转。[1063]

- “阻碍”指的是干扰计算机系统正常运转的任何行为。[1064] 这一条款的应用仅限于通过上述其中一种行为而实施的阻碍案件。

下面所列这些以不利方式影响计算机系统正常运转的行为是决定性的。[1065]

- “输入”这一术语既不是由《公约》本身定义的，也不是由《公约》的起草者定义的。至于以下事实，即传输在第 5 条中作为一种额外的行为来提及，“输入”这一术语可以被定义为任何涉及使用输入接口来向计算机系统传输信息的行为，而“传递”这一术语涵盖了伴随数据远程输入而出现的行为。[1066]
- “破坏”和“毁坏”这两个术语是有重叠的，在《解释报告》中，相对于第 4 条，《公约》的起草者将其定义为对数据和程序的信息内容信息的完整性作了不利修改。[1067]
- “删除”这一术语也是由《公约》和《解释报告》的起草者相对于第 4 条定义的，包括从存储介质中移去信息的行为。[1068]
- “更改”这一术语包括对现有数据的修改，不一定降低了数据的适用性。[1069]
- “限制”计算机数据指的是影响到可访问介质之人的数据可用性的行为，在这一行为下，信息以一种不利的方式进行保存。[1070]

此外，条款的适用仅限于“严重”阻碍的案件。各方的责任是确定一个实施标准，以便将阻碍认定为严重。[1071] 根据国家法律，可能的限制包括最小幅度的破坏，以及对攻击重要计算机系统的行为进行定罪的限制。[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 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.

针对垃圾邮件的条款应用：

对垃圾电子邮件[1073]问题能否依据第 5 条进行解决的问题进行了讨论，原因是垃圾邮件可以使计算机系统过载。[1074]起草者明确声明，垃圾邮件不一定导致“严重”阻碍，而且“对这一行为应当只在通信被有意且严重阻碍的情况下才进行定罪”。[1075]起草者还指出，各方可以根据它们自身的国家法律，采用不同的方法来对阻碍行为进行定罪，[1076]比如，通过对干扰管理的违法行为进行定罪或者进行制裁。[1077]

心理因素：

与《网络犯罪公约》定义的所有其他违法行为一样，第 5 条要求违法者是有意实施了违法行为。[1078]这包括有意实施了所列举的其中一种违法行为，以及有意严重阻碍计算机系统的正常运转。

《公约》没有包含对“有意”这一术语的定义。在《解释报告》中，起草者指出，对“有意”应在国家层面上进行定义。[1079]

未获授权：

违法行为需要是“未获授权”实施的。[1080]如之前所指出的那样，网络管理员以及负责测试计算机系统保护措施的安全公司，害怕对其工作可能进行定罪。[1081]这些专业人士经计算机系统所有者许可后开展工作，因此是合法行为。此外，《公约》的起草者还明确提出，经所有者授权而对计算机系统的安全性进行测试，不属于“未获授权”。[1082]

[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.”

限制与保留：

与第 2 条至第 4 条不同，第 5 条不包含在国家法律的实施过程中限制对该条款应用的明确的可能性。尽管如此，各方的责任是确定违法行为的严重程度，这使得它们可能对该条款的应用进行限制。在欧盟关于信息系统攻击的框架[1083]决定中可以找到一种类似的方法。[1084]

《英联邦计算机以及与计算机有关的犯罪的示范法》：

在 2002 年版的《英联邦示范法》第 7 节中可以找到一种与《网络犯罪公约》第 5 条相一致的方法。[1085]

> **第 7 节**
>
> （1）无论何人，没有合法或正当的理由，有意或鲁莽地实施了下列任何一种行为；
>
> （a）阻碍或干扰了计算机系统的运转；或者
>
> （b）阻碍或干扰了合法使用或操作计算机系统的人；
>
> 即在实施一种可处罚的违法行为，在定罪时，处以不超过[一定期限]的监禁，或者不超过[一定数量]的罚款，或者两项并罚。
>
> 在第（1）小节中，与计算机系统有关，“干扰”包括但不限于：
>
> （a）切断计算机系统的电源；以及
>
> （b）导致对计算机系统的电磁干扰；以及
>
> （c）通过任何手段毁坏计算机系统；以及
>
> （d）输入、删除或更改计算机数据；

与《公约》的主要差别在于以下事实：根据《英联邦示范法》第 7 节，即使是鲁莽的行为也将被定罪。采用这种方法，《示范法》甚至超出了《网络犯罪公约》的要求。另一个差别在于以下事实：相比《网络犯罪公约》第 5 条，《英联邦示范法》第 7 节中“干扰”的定义列出了更多的违法行为。

《斯坦福公约》草案：

非正式的[1086] 1999 年版的《斯坦福公约》草案包含了一个对干扰计算机系统的违法行为进行定罪的条款。

[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,

条款：

第 3 条

1. 根据这一《公约》，如果任何人在未获得法律认可的授权、许可或同意的情况下非法且有意地从事以下任何行为，即认为是在实施违法行为：

（a）本着以下目的，即导致或明知此类行为将导致上述网络系统或另一个网络系统如其所预期的那样停止运转，或者不按该网络系统拥有者所预期的那样运行，来创建、存储、更改、删除、传输、转移、误传、操纵或干扰网络系统中的数据或程序，根据本《公约》，将被视为非法行为；

包括的违法行为：

《网络犯罪公约》、《英联邦示范法》与《公约》草案方法之间的主要区别在以下事实，即《公约》草案涵盖任何操纵计算机系统的行为，而《网络犯罪公约》和《英联邦示范法》仅限于对阻碍计算机系统正常运转的行为进行定罪。

6.1.6 色情材料

非法内容和色情内容的定罪及定罪的轻重，在国与国之间各不相同。[1087] 参与《网络犯罪公约》谈判的各签约国着重讨论了关于儿童色情的法律协调问题，并排除了对色情与淫秽材料进行更广泛的定罪。有些国家通过以下方法解决了该问题，即执行有关对通过计算机系统进行色情材料交换的行为予以定罪的条款。不过，由于缺乏标准的定义，因此若违法者是在那些不对色情内容交换行为进行定罪的国家实施其违法行为，将使执法机构难以对这些罪行展开调查。[1088]

示例：

对色情材料交换进行定罪的一个例子是德国刑法第 184 节：

第 184 节 色情作品的传播

（1）不论是谁，涉及到色情作品（第 11 节第（3）小节）：

1. 提供、给予或制作它们，使 18 岁以下的未成年人能够接触到它们；

2. 在 18 岁以下未成年人能够接触到它们的场合显示、张贴、展示或以其他方式使未成年人可以获得它们，或者使他们可以看到；

3. 将其提供给或给予商业单位以外的零售业、顾客通常不会进入的售货亭或其他销售区域中的另一个人，通过邮购业务或者商业化租赁图书店或读书会的方式来提供或给予；

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.

[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.

3a. 通过商业化出租手段或类似的商业化设施，将其提供给或给予另一个人，以供使用，18 岁以下未成年人不能接触到的和不能看到的商店除外；

4. 通过邮购业务引进它们；

5. 在 18 岁以下未成年人能够接触到的或者能够看到的场合公开提供、宣传或评价它们，或者通过正常的商业途径在商业交易之外传播这些作品；

6. 在他人未请求这样做的情况下允许另一个人获得它们；

7. 在公共的电影放映场所中放映它们，以便从该放映中得到要求的全部或主要补偿；

8. 制作、获取、供应、储存或引进它们，以便在第 1 条至第 7 条规定的情形中使用或拷贝它们，或者使另一个人能够这样使用；或者

9. 出口它们，以便向国外传播它们或者它们的复制品，违反该国适用的刑法条款，或者使公众可以接触到它们或者也可以这样使用，应处以不超过一年的监禁或一定数量的罚款。

该条款基于这样一种概念：如果没有涉及未成年人，那么对交易和以其他方式交换色情作品，不应予以定罪。[1089] 在此基础上，法律旨在保护未成年人的健康成长。[1090] 接触色情内容是否会对未成年人的健康成长造成负面影响，是一个有争议的话题。[1091] 对在成年人中交换色情作品，根据第 184 节，不会被定罪。“作品”这一术语不仅涵盖传统的作品，而且还涵盖以数字方式存储的作品。[1092] 同样地，“使未成年人可以接触到它们”不仅适用于国际互联网之外的接触方式，而且还涵盖违法者使色情内容在网站上可用的情形。[1093]

此条款之外、对任何色情内容都予以定罪的一种方法的一个例子是，2007 年版的菲律宾议院第 3777 号法律草案的第 4.C.1 节。[1094]

> **第 4.C1 节：** 与网络色情有关的违法行为 — 无损于依照共和国法案第 9208 号和共和国法案第 7610 号进行的起诉，无论何人，以任何方式，通过使用信息通信技术，例如但不限于计算机、计算机网络、电视、卫星、移动电话[…]等，广告、推介或促进网络色情活动。
>
> **第 3i 节：** 网络色情或虚拟色情 — 指的是在计算机或通信网络帮助下进行的、任何形式的性行为或性刺激。

本条款遵循一种非常广泛的方法，原因是它对任何种类的色情广告或者通过国际互联网进行的宣扬性行为的行为，一概予以定罪。由于双重犯罪原则，[1095] 采用这种广泛方法进行国际调查将会面临诸多困难。[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

6.1.7 儿童色情

国际互联网正成为交易和交换包含儿童色情的材料的主要手段。[1097] 这种发展趋势的主要原因在于国际互联网能够快速且有效地传输文件、制作和分发的成本很低，并可以以匿名方式来进行。[1098] 置于网页上的图片可以被世界范围内数以百万计的用户访问和下载。[1099] 提供色情内容或者甚至儿童色情内容的网页之所以如此“成功”，其中一个最重要的原因是国际互联网用户感到自己很少受到监视，同时可以方便地坐在家里从国际互联网上下载材料。除非用户利用匿名通信手段，否则他们认为自己是不可能被跟踪的想法是错误的。[1100] 大多数国际互联网用户不知道他们上网冲浪时会留下电子痕迹。[1101]

《欧洲理事会关于网络犯罪的公约》：

为了加强和协调对儿童的保护，使其免受性虐待，[1102] 《公约》包括一条旨在解决儿童色情问题的条款。

条款：

第 9 条 — 与儿童色情有关的违法行为

（1）当以下行为是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：

a）以通过计算机系统分发为目的而制作儿童色情材料；

b）通过计算机系统提供儿童色情材料或使儿童色情材料可用；

c）通过计算机系统分发或传播儿童色情材料；

d）通过计算机系统为自己或他人获取儿童色情材料；

e）在计算机系统或计算机数据存储介质中拥有儿童色情材料。

（2）出于上述第 1 段的目的，“儿童色情材料”这一术语应包括以下以视觉形式进行描述的色情材料：

a）有未成年人参与明确的性行为；

---

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.

[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.

b）参与明确性行为的人看起来是未成年人；

c）展示未成年人参与明确性行为的真实图像。

（3）出于上述第 2 段的目的，“未成年人”这一术语应包括 18 岁以下的所有人。不过，签约方可以要求一个更低的年龄限制，但不得小于 16 岁。

（4）各方可以全部或部分保留不应用第 1 段第 d、e 小段和第 2 段第 b、c 小段的权利。

大多数国家已对虐待儿童以及利用传统方法散布儿童色情材料的行为进行定罪。[1103] 因此，《公约》不限于缩小国家刑法的差距，[1104] — 它还需求协调各种不同的规定。[1105] 第 9 条中涵盖了三个有争议的因素：

- 涉案人员的年龄；
- 对拥有儿童色情材料行为的定罪；以及
- 虚构图片的制作或集成。[1106]

未成年人的年龄界限：

国家法律之间最重要的差别之一是当事者的年龄。有些国家根据联合国《儿童权利公约》[1107] 中关于“儿童”的定义，在它们的国家法律中将涉及儿童色情的“未成年人”定义为所有不到 18 岁的人。另一些国家将未成年人定义为 14 岁以下的人。[1108] 在 2003 年版的欧盟理事会关于与儿童性侵犯和儿童色情作斗争的《框架决定》[1109] 中以及 2007 年版的欧洲理事会关于保护儿童免遭性侵犯和性虐待的《公约》[1110] 中可以找到一种类似的方法。强调制定统一的、关于年龄国际标准的重要性，《公约》根据《联合国公约》对该术语进行了定义。[1111] 不过，认识到现有国家法律之间的巨大差异，《公约》允许各方要求采用不低于 16 岁这一不同的年龄界限。

对拥有儿童色情材料行为的定罪：

不同国家法律体系之间在对拥有儿童色情材料的定罪方面也存在差异。[1112] 对此类材料的需求可能导致在现有的基础上制作它们。[1113] 而拥有此类材料可能会怂恿对儿童的性虐待，因此起草者建

[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.

议，制止制作儿童色情材料的一种有效方法是判定拥有它们是非法的。[1114] 不过，在第 4 段中，《公约》使各方能够排除对简单拥有的定罪，而将刑事责任仅限于儿童色情材料的制作、提供和传播。[1115]

虚构图片的制作或集成：

尽管起草者寻求加强对儿童在性侵犯面前的保护，但第 2 段涵盖的法定权益更广泛。第 2（a）段直接着眼于对虐待儿童行为的保护。第 2（b）段和第 2（c）段涵盖了在不侵犯儿童权利的情况下制作的图片 — 例如，通过使用 3D 建模软件制作的图片。[1116] 对虚构的儿童色情内容进行定罪的理由在于这些图片 — 不一定对某个真正的“儿童”造成了伤害 — 但可用来诱引儿童参与此类行为。[1117]

心理因素：

与《网络犯罪公约》确定的所有其他违法行为一样，第 9 条要求违法者是有意实施了违法行为。[1118] 在《解释报告》中，起草者明确指出，《公约》不对无意中接触到儿童色情材料的行为进行定罪。“无意”尤其指的是以下情况，即违犯者偶然间打开了一个带有儿童色情图像的网页，并且尽管他立即关闭了网站，但有些图片也已保存在了临时文件夹或缓冲文件中。

未获授权：

根据《公约》第 9 条，与儿童色情有关的行为，只有当它是“未获授权”的情况下发生时，才会被起诉。[1119] 《公约》起草者没有进一步规定在哪些情况下用户的行为是经授权的行为。一般地，只有在调查犯罪案件过程中，执法机构的成员浏览儿童色情内容的行为才不属于“未获授权”。

《欧洲理事会关于保护儿童的公约》：

《欧洲理事会关于保护儿童免受性侵犯与性虐待的公约》第 20 条是对与儿童色情有关的行为进行定罪的另一方法。[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).

条款：

第 20 条 — 涉及儿童色情的违法行为

（1）当以下行为是未经授权而故意进行时，各方应采取必要的法律措施或其他措施，以确保将其判定为犯罪行为。

a）制作儿童色情内容；

b）提供儿童色情内容或使之可用；

c）散布或传输儿童色情内容；

d）为自己或为他人获取儿童色情内容；

e）拥有儿童色情内容；

f）明知通过信息通信技术可访问到儿童色情内容而去访问。

（2）出于当前条款的目的，“儿童色情内容”这一术语应指的是在视觉上描述儿童真正或模拟参与明确性行为的任何材料，或者是主要出于色情目的而描述儿童性器官的任何材料。

（3）各方可以全部或部分保留不将第 1 段第 a、e 小段应用于制作和拥有色情材料行为的权利：

— 排他地包含模拟的展示或者非实际存在儿童的真实图像；

— 涉及已经达到第 18 条第 2 段所设定之年龄界限的儿童，这些图像的制作和拥有得到了儿童的同意，且仅供其个人使用。

（4）各方可以全部或部分保留不应用第 1.f 段的权利。

包括的违法行为：

条款基于《网络犯罪公约》第 9 条，因此，在很大程度上与这一条款相当。[1121] 主要的区别在以下事实，即《网络犯罪公约》着眼于对与信息通信服务有关的行为进行定罪（“出于通过计算机系统散布的目的而制作儿童色情内容”），同时，《保护儿童公约》主要遵循一种更广义的方法（“制作儿童色情内容”），甚至涵盖了那些与计算机网络无关的行为。

尽管在所涵盖的违法行为方面存在相似之处，《保护儿童公约》第 20 条仍包含了一种《公约》未涵盖的行为。根据《保护儿童公约》第 20 条第 1f 段，将对通过计算机访问儿童色情内容的行为进行定罪。这使执法机构能够在证明违法者打开过带有儿童色情内容的网站、但无法证明违法者下载过这些材料的情况下，对违法者进行起诉。在收集证据方面存在此类困难，例如，如果违法者对其存储介质中受保护的下载文件使用加密技术，那么就会造成难以收集证据。[1122] 《保护儿童公约》的

[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/*

《解释报告》指出，对违法者只是在线观看了儿童色情图片而没有下载的情形，该条款也应适用。[1123] 一般地，打开一个网站会自动启动下载过程 — 通常是在用户不知情的情况下。[1124] 因此，《解释报告》中提到的情形只与以下情形有关，即未进行后台下载。

《英联邦示范法》：

在 2002 年版的《英联邦示范法》第 10 节中可以找到一种与《网络犯罪公约》第 9 条相一致的方法。[1125]

> **第 10 节**
>
> (1) 有意实施以下任何一种行为的人:
>
> (a) 通过计算机系统发布儿童色情内容；或者
>
> (b) 出于通过计算机系统发布它们的目的而制作儿童色情内容；或者
>
> (c) 在计算机系统中或者在计算机数据存储介质中拥有儿童色情内容；在定罪时，处以不超过[一定期限]的监禁，或者不超过[一定数量]的罚款，或者两项并罚。[1126]
>
> (2) 根据第(1) (a)或第(1) (c)段，如果人们是本着真正的科学、研究、医学或执法目的而制作了儿童色情内容，那么这是对犯罪指控的一种辩护。[1127]
>
> (3) 在本节中:
>
> "儿童色情材料"包括那些在视觉上描述以下行为的材料:
>
> a) 有未成年人参与明确的性行为;
>
> b) 参与明确性行为的人看起来是未成年人；或者
>
> c) 展示未成年人参与明确性行为的真实图像。
>
> "未成年人"指的是年龄在[x]岁以下的人。
>
> "发布"包括:

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.

[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.*

（a）散布、传输、传播、流传、交付、展示、为牟利而租借、交换、以物换物、出售或为出售而提供、出租或为出租而提供、以任何其他方式提供，或者以任何方式使之可用；或者

（b）出于实施第（a）段中所指行为的目的而拥有或保管或者控制；或者

（c）出于实施第（a）段中所指行为的目的而打印、拍照、拷贝或以任何其他方式（无论是相同的性质还是不同的性质）制作。

与《网络犯罪公约》的主要差别在于以下事实，即《英联邦示范法》不提供关于未成年人这一术语的明确定义，而是将其留给各成员国来定义年龄界限。

《斯坦福公约》草案：

非正式的[1128] 1999 年版的《斯坦福公约》草案没有包含能对通过计算机系统交换儿童色情内容进行定罪的条款。《公约》起草者指出，通常情况下，根据《斯坦福公约》草案，没有哪种类型的言论或出版物要求被视为犯罪行为。[1129] 认识到这些不同的国家方法，《公约》的起草者将其留给各成员国来决定对这方面的定罪。[1130]

6.1.8 仇恨言论、种族主义

并非所有国家都对仇恨言论进行定罪。[1131]

《网络犯罪公约》：

由于参与《网络犯罪公约》谈判的各方都未能就对此类材料进行定罪的通用条款达成一致，[1132] 因此，关于这一主题的条款集成到了《网络犯罪公约》的一个单独的《第一协议》中。[1133]

[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.

条款：

第 3 条 — 通过计算机系统散布种族主义和排外主义材料

1．当以下行为是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为，即通过计算机系统散布种族主义和排外主义材料，或者以其他方式使之可为公众所用。

2．签约方可以保留权利，不对本条款第 1 段中所定义的行为赋予刑事责任，前提是，如第 2 条第 1 段中所定义的那样，对这些材料的鼓吹、宣传或煽动其散布，与仇恨或暴力没有关联，并假定还有其他有效的补救措施可用。

3．尽管本条款第 2 段这样规定，出于在其国家法律体系中业已建立的、涉及言论自由的原则，签约方可以保留权利，不对那些存在歧视的案件应用第 1 段，但它不能提供如上述第 2 段中所指的补救措施。

第 4 条 — 因种族主义和排外主义而造成的威胁

当以下行为是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：

通过计算机系统，本着实施如其国内法律所定义的严重犯罪行为，威胁（i）以下人员，原因是他们属于某一团体，该团体带有种族、肤色、血统或国家或种族本源以及宗教的特征，如果将这些因素中的任何一个作为借口而威胁他人，（ii）带有这些特征中任何一种特征的群体。

第 5 条 — 因种族主义和排外主义而造成的侮辱

1．当以下行为是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：

通过计算机系统，公开侮辱（i）以下人员，原因是他们属于某一团体，该团体带有种族、肤色、血统或国家或种族本源以及宗教的特征，如果将这些因素中的任何一个作为借口而威胁他人，（ii）带有这些特征中任何一种特征的群体。

2．签约方或者：

a. 要求本条款第 1 段中提到的违法行为对第 1 段中提到的个人或群体产生了影响，使后者遭到仇恨、蔑视或嘲笑；或者

b. 全部或部分保留不运用本条款第 1 段的权利。

第 6 条 – 否认、完全低估、赞成种族灭绝或反人类罪行，或者为其辩护

1．当以下行为是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：

通过计算机系统散布或以其他方式使公众可以得到以下材料：否认、完全低估、赞成种族灭绝或反人类罪行，或者为其辩护，如国际法律所定义的那样，并被国际军事法庭的最终且有约束的裁定认可，国际军事法庭依据 1945 年 8 月 8 日的《伦敦协定》建立，或者被任何其他国际法庭的最终且有约束的裁定认可，此类国际法庭依据相关的国际文件建立且该方认可其管辖权。

2．一方或者：

a. 要求本条款第 1 段中提到的，否认或完全低估，意在煽动针对某个人或某个团体的仇恨、歧视或暴力，基于其种族、肤色、血统或者国家或种族起源以及宗教，将这些因素中的任何一个作为借口，或者其他行为

b. 全部或部分保留不应用本条款第 1 段的权利。

对排外主义材料进行定罪的条款，其面临的主要困难之一是在以下两方面之间保持平衡，即一方面要确保言论自由，[1134] 另一方面要防止侵犯个人或团体的权利。在《网络犯罪公约》谈判过程中，[1135] 没有详细阐述这些困难，再加上《附加协议》的签署/批准现状，[1136] 表明各国对言论自由原则不同的保护程度阻碍了法律协调过程。[1137] 尤其是对双重犯罪通用原则，[1138] 法律协调的缺失将会给跨国犯罪案件的调查带来诸多困难。[1139]

[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;

《斯坦福公约》草案：

非正式的[1140] 1999 年版的《斯坦福公约》草案没有包括对仇恨言论进行定罪的条款。《公约》起草者指出，一般地，根据《斯坦福公约》草案，没有哪种类型的言论或出版物要求被视为是有罪的。[1141] 认识到这些不同的国家方法，《公约》的起草者将其留给各成员国来决定有关这方面的定罪问题。[1142]

6.1.9 宗教违法行为

国与国之间对宗教及其符号的保护强度各不相同。[1143]

《网络犯罪公约》：

在《网络犯罪公约》各方对这一主题谈判的过程中，面临着与排外材料中所发现的相同困难。[1144] 尽管这样，参与《网络犯罪公约》《第一附加协议》条款谈判的各国，同意在两个条款中将宗教内容增加为保护对象。

条款：

第 4 条 — 因种族主义和排外主义而造成的威胁

当以下行为是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：

通过计算机系统，本着实施如其国内法律所定义的严重犯罪行为，威胁（i）以下人员，原因是他们属于某一团体，该团体带有种族、肤色、血统或国家或种族本源以及宗教的特征，如果将这些因素中的任何一个作为借口而威胁他人，（ii）带有这些特征中任何一种特征的群体。

第 5 条 — 因种族主义和排外主义而造成的侮辱

1. 当以下行为是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：通过计算机系统，公开侮辱（i）以下人员，原因是他们属于某一团体，该团体带有种族、肤色、血统或国家或种族本源以及宗教的特征，如果将这些因素中的任何一个作为借口而公开侮辱他人，（ii）带有这些特征中任何一种特征的群体。

[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.

[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.

尽管这两个条款将宗教视为一个特征，但它们没有通过定罪来保护宗教或宗教符号。两个条款对那些因为他人属于某一团体而威胁和侮辱他人的行为定罪。

国家法律的例子：

有些国家超出了这一方法，并且对与宗教问题有关的其他行为进行定罪。一个例子是巴基斯坦刑法的第 295B 节至第 295C 节。

> **295-B**：对《古兰经》的玷污等：无论何人，恶意地玷污、破坏或亵渎《古兰经》的副本或是从中摘录的文字，或者以任何不敬的方式使用它，或者出于任何非法目的，应处以终身监禁。
>
> **295-C**：对“先知”使用不敬的言论等：无论何人，使用口头或书面语言，或者通过可视的展示，或者通过直接或间接地诋毁、影射、暗讽或玷污先知穆罕默德的神圣名字（他身边和平的力量），应处以死刑或终身监禁，还应处以罚款。

至于这一条款应用的不确定性，2006 年版的《巴基斯坦电子犯罪法案》草案包含了两条着重于与国际互联网有关的违法行为的条款：[1145]

> **20. 对《古兰经》的副本进行玷污等** — 无论何人，使用任何电子系统或电子设备，恶意地玷污、破坏或亵渎《古兰经》的副本或是从中摘录的文字，或者以任何不敬的方式使用它，或者出于任何非法目的，应处以终身监禁。
>
> **21. 对“先知”使用不敬的言论等**：无论何人，使用任何电子系统或电子设备，使用口头或书面语言，或者通过可视的展示，或者通过直接或间接地诋毁、影射、暗讽或玷污先知穆罕默德的神圣名字（他身边和平的力量），应处以死刑或终身监禁，还应处以罚款。

与关于对利用国际互联网散布排外主义材料的行为进行定罪的条款一样，全球方法的主要挑战之一是，对宗教违法行为进行定罪涉及言论自由原则。[1146] 正如之前所指出的那样，对言论自由不同的保护程度阻碍了法律协调过程。[1147] 尤其是对双重犯罪通用原则，[1148] 法律协调的缺失将会给具有国际影响的案件的执行带来诸多困难。[1149]

[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;

6.1.10 非法赌博

越来越多的网站提供非法赌博，这已成为一个令人关注的问题，[1150] 原因是它们可以用来绕过某些国家中强制执行的赌博禁令。[1151] 如果服务是在不禁止在线赌博的国家中进行操作的，那么各国将难以对国际互联网赌博的运营进行定罪，以阻止其国民使用这些服务。[1152]

国家法律的例子：

《网络犯罪公约》没有包含禁止在线赌博的条款。在这方面，国家方法的一个例子是德国的《刑法》第 284 节：

示例：

> **第 284 节 未授权地组织进行赌博游戏**
>
> （1）无论何人，未获得公用当局的许可，公开组织或经营一种赌博游戏，或者使这种装备可用，应处以不超过两年的监禁或一定数量的罚款。
>
> （2）定期在俱乐部或私人派对中进行的赌博游戏，应视为是公开组织的。
>
> （3）无论何人，在第（1）小节所述的案件中，其行为：
>
> 1.是专业的；或者
>
> 2. 作为团伙的一员，而该团伙是为了持续实施此类行为而组织起来的，应处以三个月到五年的监禁。
>
> （4）无论何人，为公开赌博游戏招募人员（第（1）小节和第（2）小节），应处以不超过一年的监禁或一定数量的罚款。

这一条款旨在限制赌博成瘾 [1153] 的风险，方法是为组织此类赌博游戏定义一些程序。[1154] 它没有明确集中于与国际互联网有关的赌博游戏，但包括它们。[1155] 在这方面，它对未获得具有法定资格之公共主管部门许可而进行的非法赌博行为予以定罪。此外，它对（有意）使这种设备可用而这种设备随后用于非法赌博的人予以定罪。[1156] 对它的定罪重于对协助赌博和教唆赌博行为的定罪，违法者可能面对更高的判决。[1157]

[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.

[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 Internetglueckksspielen 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.

为了避免招惹犯罪调查，非法赌博网站的经营者可以物理地将其行为[1158]转移到那些不对非法赌博定罪的国家。[1159]此类地点转移对执法机构而言是一项挑战，原因是服务器位于其所在国的管辖范围之外，[1160]通常不会影响到国内的用户访问它。[1161]为了提高执法机构与非法赌博作斗争的可能性，德国政府将定罪延伸至用户。[1162]根据第 285 节，执法机构可以起诉参与非法赌博的用户，并且可以启动调查，即使赌博游戏的运营者身处德国之外，无法对他们进行起诉：

第 285 节 参与未获授权的赌博游戏

无论何人，参与（第 284 节）公开赌博游戏，应被处以不超过六个月的监禁，或者不超过每日 180 元的罚款。

如果违法者使用赌博网站进行洗钱活动，那么常常很难确定违法者。[1163]例如，一种防止非法赌博和洗钱活动的方法[1164]是 2005 年版的《美国非法国际互联网赌博强制法案》。[1165]

5363. 禁止接受任何用于非法国际互联网赌博的金融手段

任何从事博彩业的人都不得有意接受、与任何参与非法国际互联网赌博之人有关的

（1）延伸至或代表相关的其他人的信用或信用收益（包括通过使用信用卡而延伸的信用）；

（2）来自或代表相关的其他人的电子资金转移，或者借助、通过资金转移业务而转移的资金，或者电子资金转移、资金转移业务的收益；

（3）由相关的其他人开具或代表相关的其他人的任何支票、汇票或类似的文书，而且是在任何金融机构或通过任何金融机构而开具的或是可付的；或者

（4）任何其他形式金融业务的收益，因财政部长依据规定做出指示，涉及将金融机构作为支付者，或者代表相关的其他人或为了相关的其他人的利益，将金融机构作为金融中介。

[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.

[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.

5364. 识别和防止受限业务的政策与程序

自本小章通过之日起，在 270 天的期限结束之前，财政部长会同美国联邦储备系统的监管理事会和司法部长，应规定一系列制度，要求各指定的支付系统和所有相关的参与者，通过建立一些政策和合理的程序，来识别和防止受限的业务，设计这些政策和程序的目的是为了以任何下列方式来识别和防止受限的业务：

（1）建立一些政策和程序，它们

（A）使支付系统和涉及支付系统的任何人都能够借助授权消息中的代码或通过其他手段识别受限的业务；以及

（B）阻拦识别出的受限业务，是依据第（A）小段而制定的政策和程序的识别结果。

（2）建立一些政策和程序，以防止接受支付系统中与受限业务有关的产品和服务。

（b）在依据第（a）小节规定制度时，财政部长将：

（1）确定政策与程序的类型，包括非排他性的例子，如何认为合适，可对之进行合理的设计，以识别、阻拦或防止接受与各类受限业务有关的产品或服务；

（2）为了切合实际，允许支付系统的任何参与者选择其他可选手段来识别、阻拦或以其他方式来阻止接受与受限业务有关的、支付系统或参与者的产品或服务；以及

（3）如果财政部长发现，识别、阻拦或以其他方式阻止此类业务是不切实际的，那么考虑对有些受限业务豁免此类规定所施加的任何要求。

（c）金融业务提供商将被认为是符合第（a）小节中所规定的制度的，如果：

（1）此类人依靠并遵守指定之支付系统的政策与程序，他们是该系统的成员，或是以下工作的参与者：

（A）识别和阻拦受限业务；或者

（B）以其他方式阻止接受支付系统、成员或其他与受限业务有关的参与者的产品或服务；以及

（2）指定之支付系统的此类政策和程序符合第（a）小节所规定之制度的要求。

（d）受制于规定之制度或者依据本小章发布之命令的人，当阻拦或以其他方式拒绝办理某项业务时，应具有如下理由：

（1）这是一项受限业务；

（2）此人合理地认为这是一项受限业务；或者

（3）作为依赖支付系统之政策与程序的、指定支付系统的成员，为努力与第（a）小节所规定的制度保持一致，不应因此类行为而对任何一方负责。

（e）本节的要求将由联邦职能监管部门和联邦贸易委员会排他地执行，执行方式依照《金融服务现代化法案》第 505（a）节中所述的规定。

5366. 刑事处罚

（a）无论何人，违反第 5363 节规定之内容，将根据第 18 条处以罚款，或者处以不超过 5 年的监禁，或者两项并罚。

（b）根据本节被判有罪之人，法庭可判决终身禁止此人投资、接受或以其他方式从事博彩业，或者终身禁止发出、接收或要求用于协助博彩业投资的信息。

该法案的目的是为了应对国际互联网赌博的挑战和（跨境）威胁。[1166] 它包含两个重要的规定：首先，禁止接受任何从事博彩业之人用于非法国际互联网赌博的任何金融工具。这一条款没有管制由国际互联网赌博网站或金融机构的用户所实施的行为。[1167] 违反这一禁令可招致刑事制裁。[1168] 此外，该法案要求财政部长和美国联邦储备系统监管理事会规定一些制度，要求金融业务提供商通过合理的政策和程序，识别和阻拦与非法国际互联网赌博有关的受限业务。第二条规定不仅影响从事博彩也的人，而且一般会影响所有的金融机构。与接受从事博彩业之人用于非法国际互联网赌博的金融工具不同，金融机构一般不会面临刑事责任。至于可能与《服务贸易总协定》（GATS）[1169] 有冲突的规定的国际影响问题，目前正在研究中。[1170]

6.1.11 侮辱与诽谤

诽谤和公开发表虚假信息并非只是能在网络中实施的违法行为。但正如之前所指出的那样，匿名通信的可能性 [1171] 以及与国际互联网中大量可用信息有关的逻辑挑战 [1172]，都是支持此类违法行为的抽象要素。

这是否要求对诽谤进行定罪？对这一问题当前正在有争议地讨论着。[1173] 关于对诽谤进行定罪的考虑，尤其与“言论自由”原则可能发生的冲突有关。因此，大量的组织呼吁替换关于诽谤的刑法条款。[1174] 联合国观点和言论自由问题特别报告起草人以及关于媒体自由的 OSCE 代表表示：

[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:

"对诽谤定罪不是对言论自由的合理限制；所有涉及诽谤的刑法都应废止和替换，必要时，用合适的民法条款来替换。" [1175]

尽管有这些考虑，但一些国家[1176]已经实施了对诽谤进行定罪的刑法条款，同时也对虚假信息的公开发布予以定罪。重要的是强调，即使在那些对诽谤予以定罪的国家内，案件的数量也极不相同。在英国，2004 年全年没有人因诽谤而遭起诉，2005 年也只有一个嫌疑人因诽谤而遭起诉。[1177]德国的犯罪数据统计记录，2006 年有 187527 件诽谤案件。[1178]《网络犯罪公约》、《英联邦示范法》和《斯坦福公约》草案没有包含直接涉及这些行为的条款。

国家法律的例子：

涉及诽谤的刑法条款的一个例子是《昆士兰刑法》（澳大利亚）中的第 365 节。通过 2002 年版的《2000 年刑法诽谤修正案法案》，昆士兰重新引入了有关诽谤的刑法责任。[1179]

条款：

365 违法的诽谤 [1180]

（1）无论何人，没有合法理由，公开发表诽谤他人（相关人员）的内容 —

（a）明知该内容是虚假的，或者没有注意到内容究竟是真的还是虚的；以及

（b）旨在给相关人员或任何其他人造成严重伤害，或者没有注意到是否会给相关人员或任何其他人造成严重伤害；都是在实施不当行为。最高刑罚 — 3 年监禁。

（2）在对本节所定义的违法行为进行起诉的过程中，当且仅当第 3 小节适用时，[…] 被告之人才拥有合法的理由来发布涉及相关人员的诽谤内容。

另一个对诽谤进行定罪的例子是德国的《刑法》第 185 节：

[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: 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.

条款：

第 185 节 侮辱

对侮辱，将被处以不超过一年的监禁或一定数量的罚款，如果侮辱是借助暴力手段实施的，那么将被处以不超过两年的监禁或一定数量的罚款。

两个条款都不是仅仅针对与国际互联网有关的行为。条款的应用不限于某些通信手段，因此它可以涵盖那些在网络中实施的行为，以及在网络外实施的行为。

6.1.12 垃圾邮件

在所有的电子邮件中，多达 75%[1181] 的电子邮件被报告是垃圾电子邮件，[1182] 鉴于这一事实，对是否需要对垃圾电子邮件进行刑事制裁进行了激烈讨论。[1183] 用于解决垃圾邮件问题的国家法律解决方案各不相同。[1184] 垃圾邮件为什么仍然是一个问题？其中一个主要原因是，过滤技术仍无法识别和阻拦所有的垃圾电子邮件。[1185] 保护措施仅仅针对主动发送的电子邮件提供了有限的保护措施。

2005 年，OECD 发布了一份报告，对垃圾邮件对发展中国家的影响进行了分析。[1186] 报告指出，来自发展中国家的代表常常表达这样的观点，即他们国家的国际互联网用户正受到越来越严重的、来自垃圾邮件和网络滥用的影响。对报告的结果进行分析可以证明，代表们的看法是正确的。由于资源更为有限、更为昂贵，与西方发达国家相比，发展中国家的垃圾邮件问题证明要严重得多。[1187]

不过，不仅仅在识别垃圾邮件方面存在很多困难。在接收者不期望收到、但合法发送的电子邮件与那些非法发送的电子邮件之间进行区分，也是一项挑战。当前基于计算机传输（包括电子邮件和 VoIP）的发展趋势，突显了保护通信不受攻击的重要性。如果垃圾邮件超过一定的级别，那么它们可能严重阻碍对信息通信技术的使用，并降低用户的生产率。

《网络犯罪公约》：

《网络犯罪公约》没有明确对垃圾邮件予以定罪。[1188] 起草者建议，对这些行为的定罪应限于严重和有意阻碍通信的行为。[1189] 这一方法没有着重于非请求的电子邮件，而着重于垃圾邮件对计算

[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

机系统或网络的影响。基于《网络犯罪公约》的法律方法，与垃圾邮件作斗争可能只能基于对计算机网络和系统的非法干扰：

> **第 5 条 — 系统干扰**
>
> 当通过输入、传递、破坏、删除、毁坏、更改或限制计算机数据等行为，故意而未经授权地严重阻碍计算机系统的正常运转时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为。

《斯坦福公约》草案：

非正式的[1190] 1999 年版的《斯坦福公约》草案没有包括对垃圾邮件进行定罪的条款。与《网络犯罪公约》一样，《斯坦福公约》草案只对有意造成目标系统干扰的垃圾邮件违法行为进行定罪。

国家法律的例子：

这限制了在以下案件中对垃圾邮件的定罪，即垃圾电子邮件的数量对计算机系统的处理能力产生了严重影响。对影响商务有效性、但不一定影响计算机系统的垃圾电子邮件，可能不会被起诉。因此，许多国家采用一种不同的方法。一个例子是美国的法律 — 18 U.S.C § 1037。[1191]

> **§ 1037. 与电子邮件有关的欺诈和相关行为**
>
> (a) 一般地 — 无论何人，从事或影响到国与国之间的贸易或者对外贸易，明知 —
>
> (1) 未获授权而访问一台受保护的计算机，并且从该台计算机或者通过该台计算机，有意地传送多份商务电子邮件消息；
>
> (2) 使用一台受保护的计算机，来转发或重发多份商务电子邮件消息，旨在欺骗或误导邮件接收者，或者源自此类消息的任何国际互联网接入服务，
>
> (3) 对多份商务电子邮件消息中的标题信息做实质性修改，并有意传送此类消息，
>
> (4) 使用经对实际注册者身份进行实质性篡改后的信息来注册五个或更多个的电子邮件账号或者在线用户账号或者两个或更多个域名，并且有意地用此类账号或域名的某种组合来传送多份商务电子邮件消息，或者
>
> (5) 虚假地将自己介绍为注册者或者 5 个或更多个国际互联网协议地址注册者权益的合法继承者，并且有意第从此类地址传送多份商务电子邮件消息，

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."

[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.

或者密谋这样做，将被处以第（b）小节所规定的处罚。

（b）处罚 — 依据第（a）小节，对违法行为的处罚是 —

（1）一定数量的罚款，或者不超过 5 年的监禁，或者两项并罚，如果 —

（A）根据美国或任何州的法律，这些违法行为的实施促进了任何重罪；或者

（B）被告之前曾根据本节或第 1030 节被判有罪，或者根据任何一州的法律，因为涉嫌发送多份商务电子邮件消息或者未获授权访问计算机系统而被判有罪；

这一条款由 2003 年版的《CAN 垃圾邮件法案》来实施。[1192] 该法案旨在创建一个单独的国家标准，以便控制商务电子邮件。[1193] 它适用于商务电子消息，但不适用于那些与业务以及现有商业关系有关的消息。管制方法要求商务电子消息包括指明请求发送，包括自愿退出指令和发送者物理地址。[1194] 18 U.S.C. § 1037 对垃圾电子邮件的发送者定罪，尤其当他们篡改电子邮件的报头信息以绕过过滤技术时。[1195] 此外，该条款还对未获授权访问受保护计算机系统并启动多份商务电子邮件消息发送的行为予以定罪。

6.1.13 设备误用

另一个严重的问题是设计用来实施犯罪的软件和硬件工具的可用性。[1196] 除了“黑客设备”的大量扩散，使未获授权的用户能够访问计算机系统的密码交换也是一项严峻的挑战。[1197] 这些设备的可用性及其潜在的威胁，使难以仅仅关注于对使用这些工具来实施犯罪的行为进行定罪。除了“违法行为的企图”之外，大多数国家刑法体系有一些针对准备和制造这些工具的行为进行定罪的条款。与此类设备传播行为作斗争的一种方法是，对工具的制造予以定罪。一般地，这种定罪 — 通常伴随广泛的刑事责任前移 — 限于最严重的罪行。特别是在欧盟的法律中，存在一些趋势，欲将定罪向不太严重的违法行为的准备活动延伸。[1198]

《网络犯罪公约》：

考虑到欧洲理事会的其他举措，《公约》的起草者为以下特定的违法行为确立了一种独立的非法行为，即出于破坏计算机系统或数据的机密性、完整性和可用性的目的，误用某些设备或访问数据。[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“.

条款：

第 6 条 — 设备误用

（1）当以下行为是故意而未经授权地进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：

（a）制作、销售、为使用而取得、输入、发行或以其他方式使之可用于：

（i）被设计或改装成主要用于依据上述第 2 条至第 5 条确定之任何违法行为的装置，包括计算机程序；

（ii）用之可以进入整个计算机系统或任何部分的计算机密码、访问密码或类似数据，旨在用之实施第 2 条至第 5 条中所确定的任何违法行为；以及

（b）拥有上述第 a）i 或 ii 段中所提及的物品，旨在将其用于实施第 2 条至第 5 条中所确定的任何违法行为。签约方可以通过法律手段规定在需担负刑事责任之前能拥有此类物品的数量。

（2）当本条款第 1 段中所提及的制作、销售、为使用而取得、输入、分发或者以其他方式使之可用或拥有的行为不是用于实施本《公约》第 2 条至第 5 条所规定之违法行为而是在授权后用于测试或保护计算机系统时，本条款将不被解释为施加刑事责任。

（3）假如权利的保留不涉及本条款第 1 a.ii 段中所提及的销售、分发或者以其他方式使物品可用，各方可以保留不应用本条款第 1 段的权利。

包括的对象：

第 1（a）段确定了设计用于实施和推动网络犯罪的设备，[1200] 以及能够实现对计算机系统访问的密码。

- “装置”这一术语涵盖用于实施上述违法行为之一的、基于硬件和软件的解决方案。例如，《解释报告》中提到的软件，诸如病毒程序或者为实现对计算机系统的访问而设计或改编的程序。[1201]
- “计算机密码、访问密码或类似的数据”不同于设备，它们不执行操作而是访问密码。在这一背景中讨论的一个问题是，条款是否涵盖公布系统弱点。[1202] 与典型的访问密码系统不同，弱点并不一定使别人能够迅速访问计算机系统，但使违法者能够利用它们来成功攻击计算机系统 。

包括的违法行为：

《公约》对众多违法行为予以定罪。除了对制作进行定罪之外，它还对销售、为使用而取得、输入、分发或以其他方式是装置和密码可用的行为进行制裁。在欧洲关于协调版权 [1203] 的法律中可以

[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.
[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

找到一种类似的方法（限于设计用来绕过技术措施的装置），同时，许多国家已经在其刑法中执行了类似条款。[1204]

- “分发”涵盖主动向他人转运（转发）装置或密码的行为。[1205]
- “销售”指的是为获得金钱回报或其他报酬而涉及装置和密码销售的行为。
- “为使用而取得”涵盖与主动获取密码和装置有关的行为。[1206] 取得行为与此类工具的使用相关，这一事实一般要求违法者具有以下意图，即在取得这些工具后，将其用于“实施第 2 条至第 5 条所规定之违法行为”，这超出了“正常的”意图。

输入包括从外国获取装置和访问密码的行为。[1207] 结果是，输入此类工具并销售它们的违法者，甚至可以在他们提供工具之前就遭到起诉。事实是，只有当获得此类工具并用于可疑目的时才会被起诉，若工具的销售或使用不存在《网络犯罪公约》第 6 条所涵盖的意图，则不会被起诉。

---

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.

“使之可用”指的是以下行为，通过它可使其他用户可以使用这些物品。[1208] 《解释报告》建议，“使之可用”这一术语也可以用来涵盖创建或编辑超链接，以方便对此类装置的使用。[1209]

双重使用工具：

与欧盟趋向协调版权 [1210] 的方法不同，条款不仅适用于那些专门设计用来便利网络犯罪实施的装置 — 《公约》还涵盖那些通常用于合法目的的装置，在这种情况下，违法者的特定意图是实施网络犯罪。在《解释报告》中，起草者建议，将装置限定在专门设计用来实施网络犯罪的装置上过于狭窄了，可能导致在证明犯罪诉讼中出现难以克服的困难，使该条款事实上无法适用或者只能对少数情形适用。[1211]

为确保实现对计算机系统的适当保护，专家们使用和拥有各种各样的软件工具，使自己能够集中于执法。《公约》以三种方式审视了这些利害关系：[1212]

- 它使第 6 条第 1（b）段中的各方能在以下方面作出一些保留，即在确定刑事责任之前规定可以拥有此类物品的最大数量。
- 除了这一点，对拥有这些装置的行为定罪，限于要求拥有者具备利用此类装置实施《公约》第 2 条至第 5 条中所规定之违法行为的意图。[1213] 《解释报告》指出，将这种特殊的意图纳入，是为了“避免对出于合法目的而制造和销售此类装置的行为出现过度定罪的危险，比如，为了对付针对计算机系统的攻击等。” [1214]
- 最后，《公约》的起草者在第 2 段中明确声明，条款不包括为授权测试或为保护计算机系统而制造此类工具的行为，原因是条款已经涵盖未获授权行为。

[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.

[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’.”

对拥有行为的定罪：

第 1（b）段进一步强化了第 1（a）段中的规定，方法是，如果拥有装备或密码的行为与实施网络犯罪的意图有关，那么予以定罪。对拥有此类工具进行定罪是有争议的。[1215] 第 6 条不限于专门设计用于实施犯罪的工具，而对之定罪的反对者担心，对拥有此类装置的行为进行定罪，可能对系统管理员和网络安全专家构成不可接受的风险。[1216] 《公约》使各方能够在附带刑事责任之前要求拥有一定数量的此类物品。

心理因素：

与《网络犯罪公约》中所定义的所有其他违法行为一样，第 6 条也要求违法者是有意实施违法行为。[1217] 除了所涵盖之行为的普通意图之外，《网络犯罪公约》第 6 条还要求具备额外的特殊意图，即将装置用于实施《网络犯罪公约》第 2 条至第 5 条中所确定的任何一种违法行为。[1218]

未获授权：

与上面讨论的条款一样，这些行为必须是“未获授权”而实施的。[1219] 至于担心该条款可能被用来对自我保护措施之内的软件工具的合法操作行为进行定罪，《公约》的起草者指出，此类行为不会被视为“未获授权”。[1220]

限制与保留：

由于对是否需要对拥有这种装置的行为进行定罪存在争议，因此《公约》提供了对第 6 段第 3 段（除了第 1（b）段第 2 句）的复杂的保留选择方案。如果签约方使用这种保留权利，那么它可以排除对拥有这类工具行为的定罪以及对大量依据第 1（a）段认为有罪的违法行为的定罪 — 例如，制造此类装置。[1221]

《英联邦示范法》：

在 2002 年版的《英联邦示范法》第 9 节中可以找到一种与《网络犯罪公约》第 6 条相一致的方法。[1222]

[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.
[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

第 9 节

（1）某人实施违法行为，如果此人：

（a）没有合法或正当的理由，有意或鲁莽地制作、销售、为使用而取得、输入、输出、发行或以其他方式利用：

（i）设备，包括计算机程序，经设计或改装用于实施如第 5、6、7 或 8 节所述的违法行为；或者

（ii）计算机密码、访问密码或类似数据，用之可以进入整个计算机系统或任何一部分；

意图是任何人都可以用之来实施如第 5、6、7 或 8 节所述的违法行为；或者

（b）拥有一件第 i 小或 ii 小段中提及的物品，意图是任何人都可以用之来实施如第 5、6、7 或 8 节所述的违法行为。

（2）被证明犯有本节中所述之罪行的人，处以不超过[一定期限]的监禁，或者不超过[一定数量]的罚款，或者两项并罚。

与《网络犯罪公约》的主要区别在以下事实，即《英联邦示范法》对鲁莽行为进行定罪。在对《英联邦示范法》进行谈判的过程中，就对拥有此类设备的行为进行定罪的条款的进一步修正意见进行了讨论。专家小组建议，对拥有多个此类物品的违法者进行定罪。[1223] 加拿大提出了一种不预先确定物品数量而进行定罪的类似方法。[1224]

《斯坦福公约》草案：

非正式的 [1225] 1999 年版的《斯坦福公约》草案包括了一条对与某些非法设备有关的行为进行定罪的条款。

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.*

[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.

第 3 条 — 违法行为

1. 根据这一《公约》，如果任何人在未获得法律认可的授权、许可或同意的情况下非法且有意地从事以下任何行为，即认为是在实施违法行为：

[...]

(e) 制作、销售、使用、公开或以其他方式发行任何设备或程序，旨在实施本《公约》第 3 条和第 4 条中所禁止的任何行为；

《公约》起草者指出，通常情况下，根据《斯坦福公约》草案，没有哪种类型的言论或出版物要求被视为犯罪行为。[1226] 其作出的唯一例外与非法设备有关。[1227] 在这一背景下，起草者强调，定罪应仅限于提到的行为，比如，在对系统弱点进行讨论时未涵盖的行为。[1228]

6.1.14 与计算机有关的伪造

涉及与计算机有关的伪造的犯罪诉讼过去很少见，原因是大多数法律文件都是有形文件。随着数字化的发展，这种情形正在发生变化。[1229] 朝数字化文件发展的趋势，得到了为其使用创建法律背景的支持，例如，通过在法律上对数字签名的认可。此外，针对与计算机有关的伪造的条款，在与“网络钓鱼”作斗争的过程中发挥着重要作用。[1230]

《网络犯罪公约》：

大多数刑法体系都对伪造有形文件予以定罪。[1231] 《公约》起草者指出，教条式的国家法律方法结构正在改变。[1232] 一种概念是基于文件作者的真实性，而另一种概念是基于声明的真实性。起草

[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 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.

者决定执行最低的标准，并保护电子数据的安全性和可靠性，方法是制定一种平行于传统有形文件伪造的违法行为，以填补刑法可能不适用于以电子方式存储的数据的空白。[1233]

条款：

> **第 7 条 — 与计算机有关的伪造行为**
>
> 当以下行为是故意而未经授权地进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：输入、更改、删除或限制计算机数据，以产生虚假的数据，意图是使之看起来像是合法的，或者可用于合法目的，而不管此数据是否直接可读和可理解。在附带犯罪责任之前，签约方可以规定罪行成立的欺骗意图或类似的不诚实意图。

包括的违法行为：

与计算机有关的伪造，其目标是数据 — 不管它们是否是可直接可读的和/或可理解的。《公约》[1234] 将计算机数据定义为“事实、信息或概念的某种表述，它以一种适于在计算机系统中进行处理的形式存在，包括适于促使计算机系统执行某种功能的程序”。该条款不仅仅指的是作为上述其中一种行为目标的计算机数据。此外，还有必要包括导致不真实数据的各种行为。

第 7 条要求 — 至少在心理因素方面 — 数据相当于公共或私人的文件。这意味着数据必须是法律上相关的 [1235] — 对不能用于合法目的的数据的伪造，没有包括在这一条款中。

1) 包括的违法行为：

- “输入”数据 [1236] 必须与制作一份虚假的有形文件相对应。[1237]
- “更改”这一术语指的是对现有数据进行修改。[1238] 《解释报告》特别指出了各种不同的更改和部分更改。[1239]
- “限制”计算机数据这一术语指的是影响数据可用性的行为。[1240] 在《解释报告》中，起草者特别提到了隐瞒或隐藏数据的行为。[1241] 比如，这一行为可以通过在自动创建电子文件期间阻碍某些来自数据库的信息来实施。
- “删除”这一术语对应第 4 条中的术语定义，涵盖移去信息的各种行为。[1242] 《解释报告》只提到了从数据介质中移去数据。[1243] 但条款的范围强烈支持拓宽“删除”的定义。基于这种更

[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.
[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.

加广义的定义，“删除”行为可以通过移除整个文件来实施，或者可以通过部分删去文件中的信息来实施。[1244]

心理因素：

与《网络犯罪公约》所定义的所有其他违法行为一样，第 3 条要求违法者有意实施了违法行为。[1245]《公约》没有包含对“有意”这一术语的定义。在《解释报告》中，起草者指出，对“有意”应在国家层面上进行定义。[1246]

未获授权：

只有当伪造行为是“未获授权”时实施的，才可根据《公约》第 7 条予以起诉。[1247]

限制与保留：

第 7 条还提供了作出保留以便限制定罪的可能性，方法是要求在界定刑事责任之前需具备额外的因素，如诈骗的意图。[1248]

《英联邦示范法》：

2002 年版的《英联邦示范法》没有包含对与计算机有关的伪造进行定罪的条款。[1249]

《斯坦福公约》草案：

非正式的 [1250] 1999 年版的《斯坦福公约》草案包括一条对与伪造计算机数据有关的行为进行定罪的条款。

[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.
[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.

第 3 条 – 违法行为

1. 根据这一《公约》，如果任何人在未获得法律认可的授权、许可或同意的情况下非法且有意地从事以下任何行为，即认为是在实施违法行为：

[...]

(b) 出于以下目的以及为了产生相应的不良效应，即提供错误信息，以便对个人或财产造成实质性损坏，来创建、存储、更改、删除、传输、转移、误传、操纵或干扰网络系统中的数据或程序；

[...]

与《网络犯罪公约》第 7 条的主要区别在以下事实，即第 3 1b）条不是集中于纯粹的操纵数据，而是要求对计算机系统的干扰。《网络犯罪公约》第 7 条不要求此类行为，而只要违法者的意图是希望被人认为是合法的或者其行为看起来像是出于合法的目的就足够了。

6.1.15 身份盗用

考虑到媒体的覆盖范围、[1251] 在该领域的最新调查结果 [1252] 以及大量的法律和技术出版物，[1253] 将身份盗用描述成一种普遍现象看起来并不为过。[1254] 尽管这种现象存在于世界各地，但并非所有国家都已在其国家刑法体系中执行了对所有涉及身份盗用的行为进行定罪的条款。欧盟委员会最近声明，对身份盗用，尚未在所有欧盟成员国中都予以定罪。[1255] 该委员会表明了自己的立场，即“如果所有成员国都对身份盗用进行定罪，那么欧盟的执法合作将更加紧密”，委员会还宣布，它将立即着手进行磋商，以评估该法律是否恰当。[1256]

在与身份盗用作斗争的过程中，相比现有的法律手段，存在许多问题，其中之一是它们存在巨大差异。[1257] 现有方法之间唯一一致的因素是，被判有罪的行为与下列各阶段中的一个或多个阶段有关：[1258]

- 阶段 1：获取与身份有关的信息的行为；
- 阶段 2：拥有或传输与身份有关的信息的行为；
- 阶段 3：将与身份有关的信息用于犯罪目的的行为。

[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.

[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.

根据这种观察，对身份盗用进行定罪，一般有两种系统的方法：

- 制定一条对获取、拥有和使用与身份有关信息（出于犯罪目的）的行为进行定罪的条款。
- 对与获取身份相关信息的典型行为（如非法访问、制作和散布恶意软件、与计算机有关的伪造、数据刺探和数据干扰）以及与拥有和使用此类信息相关的行为（如与计算机有关的欺诈）分别进行定罪。

单一条款方法示例：

最著名的单一条款方法的例子是 18 U.S.C. § 1028(a) (7)和 18 U.S.C. 1028A(a) (1)。条款涵盖众多与身份盗用有关的违法行为。在这种方法中，定罪不限于某一阶段，而是涵盖上述的全部三个阶段。尽管这样，重要的是强调指出，条款没有涵盖所有与身份盗用有关的活动 — 尤其是对那些是受害者而不是违法者在行动的情况。

1028. 与身份识别文件、身份验证特征和信息有关的欺诈行为及相关活动

（a）无论何人，在本节中（c）小节所述的情形下 —

（1）有意且未获得合法授权而制作身份识别文件、身份验证特征或者虚假的身份识别文件；

（2）有意传输身份识别文件、身份验证特征或者虚假的身份识别文件，明知此类文件或特征是窃取的或未获得合法授权而制作的；

（3）本着非法使用的意图而有意拥有，或者非法传输 5 个或更多个身份识别文件（不同于那些拥有者合法使用而发行的）、身份验证特征或者虚假的身份识别文件；

（4）有意拥有身份识别文件（不同于那些拥有者合法使用而发行的）、身份验证特征或者虚假的身份识别文件，本着将此类文件或特征用于在美国境内实施诈骗的意图；

（5）有意制作、传输或拥有一种文件制作工具或身份验证特征，本着以下意图，即此类文件制作工具或身份验证特征将用于制作虚假的身份识别文件，或者用于制作另一种文件制作工具或身份验证特征，它们也将用于同样目的；

（6）有意拥有身份识别文件或身份验证特征，它们是或者看起来是一种在美国可用的身份识别文件或身份验证特征，它们是窃取的或未获得合法授权而制作的，且明知此类文件或特征是窃取的或未获得合法授权而制作的；

（7）未经合法授权有意传输、拥有或使用他人的身份证明方法，旨在实施、辅助实施或教唆实施非法活动或者连同任何非法活动一起实施，该活动触犯了联邦法律或者根据任何适用的州法律或当地法律构成了重罪；或者

（8）有意传输虚假或真实的身份验证特征，以便在虚假的身份识别文件、文件制作工具或者身份识别方法中使用；

将处以本节第（b）小节中所述的处罚。

1028A. 严重的身份盗用行为

（a）违法行为 —

（1）一般地 — 无论何人，在实施第（c）小节所列举之任何重罪以及涉及这一重罪时，未经合法授权而有意传输、拥有或使用他人的身份识别方法，除了此类重罪应获得的刑罚之外，还将被判处为期 2 年的监禁。

阶段 1：

为了实施与身份盗用有关的犯罪活动，违法者需要拥有与身份相关的数据。[1259] 通过对本着犯罪意图而“传输”身份识别方法的行为进行定罪，这些条款以非常广泛的方式对与第 1 阶段有关的行为进行定罪。[1260] 由于这些条款着重于传输行为，因此它们没有涵盖由违法者在开始传输过程之前实施的违法行为。[1261] 其他一些可以用来从受害者处获取与计算机身份有关的数据的违法行为，如发送网络钓鱼邮件和设计恶意软件等， 没有包括在 18 U.S.C. § 1028(a) (7)和 18 U.S.C. 1028A(a) (1)中。

阶段 2：

通过对本着实施犯罪的意图而拥有的行为进行定罪，条款再次采用了一种广泛的方法来对与第 2 阶段有关的行为进行定罪。这尤其包括以下违法行为，即拥有与身份有关的信息的目的是为了之后用它们来实施一种与身份盗用有关的、典型的违法行为。[1262] 拥有与身份有关的数据而无意使用它们，则不在条款的覆盖范围内。[1263]

阶段 3：

通过对本着实施犯罪的意图而“使用”的行为进行定罪，条款涵盖了与第 3 阶段有关的违法行为。如上所述，18 U.S.C. § 1028(a) (7)没有涉及特定的违法行为（如欺诈）。

多种条款方法示例：

《网络犯罪公约》与单一条款方法（如美国方法）之间的主要区别在以下事实，即《公约》没有定义一种非法使用身份相关信息的单独的网络违法行为。[1264] 类似于对获取身份相关信息的违法行为进行定罪的情形，《公约》没有涵盖与非法使用个人信息有关的、所有可能的行为。

阶段 1：

在第 1 阶段中，《网络犯罪公约》 [1265] 包含许多对与国际互联网有关的身份盗用行为进行定罪的条款。特别是以下三条：

[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.

[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

- 非法访问（第 2 条）；[1266]
- 非法截获（第 3 条）；[1267]
- 数据干扰（第 4 条）；[1268]

考虑到违法者可以获得数据的各种各样可能性，有必要指出，并未涵盖第 1 阶段中所述的所有可能的行为。常常与身份盗用第 1 阶段有关、但未包括在《网络犯罪公约》中的违法行为的一个例子是数据刺探。

阶段 2：

在获取信息以及将其用于犯罪目的之间发生的违法行为，几乎未被《网络犯罪公约》所涵盖。对于与身份有关的信息，尤其不可能通过依据《公约》所规定的条款来对销售此类信息的行为进行定罪，就可以阻止与身份信息有关的黑市日益发展壮大。

阶段 3：

《欧洲理事会关于网络犯罪的公约》定义了大量与网络犯罪有关的违法行为。其中的一些违法行为是作案者使用与身份有关的信息来实施的。一个例子是与计算机有关的欺诈，它常常在身份盗用的背景下被提及。[1269] 关于身份盗用的调查指出，大多数以非法手段获取的数据都被用来实施信用卡欺诈。[1270] 如果信用卡欺诈是在线实施的，那么有可能根据《网络犯罪公约》第 8 条来起诉作案者。其他可通过使用身份相关信息来实施的违法活动，如果这些信息是过去获取的、且未在《公约》中提及，那么不在该法律框架的覆盖范围内。如果违法者本着隐藏其身份的目的而使用与身份有关的信息，那么要起诉他尤其是不可能的。

6.1.16 与计算机有关的欺骗

欺骗是网络空间里一种普遍存在的犯罪。[1271] 在国际互联网之外，它也是一种普遍问题，因此，大多数国家法律包含对此类违法行为进行定罪的条款。[1272] 不过，将现有条款用于与国际互联网有关的案件存在一些困难，原因是传统的国家刑法条款是基于个人的欺骗。[1273] 事实上，在许多借助

---

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.

[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,

国际互联网实施的欺骗案件中，正是计算机系统对违法者的行为进行响应。如果传统的打击欺骗的刑法条款没有涵盖计算机系统，那么有必要对国家法律进行更新。[1274]

《网络犯罪公约》：

通过提供一条针对与计算机有关的欺骗的条款，《公约》寻求对任何不当的、对数据处理过程进行操纵的行为予以定罪，该行为意在影响财产的非法转移。[1275]

条款：

> **第 8 条 — 与计算机有关的欺诈行为**
>
> 当以下对他人财产造成了损失的违法行为是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为。
>
> a. 任何输入、更改、删除或限制计算机数据的行为；
>
> b. 任何干扰计算机系统正常运转的行为，这些行为本着欺骗性的或不诚实的意图，在未经授权的情况下为自己或他人获取经济利益。

包括的违法行为：

第 8 条 a）包含了一个与计算机有关的欺诈行为最为相关的违法行为清单。[1276]

- “输入”计算机数据包括所有种类的输入操纵，比如向计算机输入不正确的数据、操纵计算机软件以及其他干扰数据处理过程的行为。[1277]

---

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.

[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.

- “更改”这一术语指的是修改现有数据。[1278]
- “限制”计算机数据这一术语指的是影响数据可用性的行为。[1279]
- “删除”这一术语对应第 4 条中的术语定义，涵盖移去信息的各种行为。[1280]

除了列举违法行为之外，第 8 条 b）包含一条普通条款，该条款对与欺骗有关的“干扰计算机系统的正常运转”行为予以定罪。该普通条款添加到了包括的违法行为的列表中，以便给条款的进一步完善留下空间。[1281]

《解释报告》指出，“干扰计算机系统的正常运转”涵盖以下行为，如操纵硬件、限制打印资料、影响数据记录与流动，或者影响程序运行次序等。[1282]

经济损失：

依据大多数国家刑法，犯罪行为必须造成经济损失。《公约》采用了一种类似的概念，仅对那些操纵行为予以定罪，这些操纵行为对他人的财产造成了直接的经济损失或所有权损失，包括金钱损失、有形和无形的经济价值损失等。[1283]

心理因素：

与其他列举的违法行为一样，《网络犯罪公约》第 8 条要求违法者有意实施违法行为。这种意图指的是有意操纵以及有意造成经济损失。

此外，《公约》要求违法者的行为具有欺骗或不诚实意图，以便为自己或他人获取经济利益或其他利益。[1284] 作为不承担刑事责任行为的例子，由于缺少特殊意图，《解释报告》提到了源自市场竞争的商业作法，这些作法可能给某人造成经济损失但给另一人带来经济利益，但它们的实施不具备欺骗或不诚实意图。[1285]

未获授权：

只有当访问是“未获授权”时，才能根据《公约》第 8 条对与计算机有关的欺骗行为进行起诉。[1286] 这包括要求经济利益的获得是未获授权的。《公约》起草者指出，根据相关各方签订的有效合同而实施的行为，不被视为未获授权。[1287]

[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.
[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.

《英联邦示范法》：

2002 年版的《英联邦示范法》没有包括对与计算机有关的欺骗进行定罪的条款。[1288]

《斯坦福公约》草案：

非正式的 [1289] 1999 年版的《斯坦福公约》草案没有包括对与计算机有关的欺骗进行定罪的条款。

6.1.17 版权犯罪

在发行版权保护内容过程中模拟到数字的转换，标志着在版权侵权中出现了转折点。[1290] 对音乐和视频作品的复制，过去一直限于对模拟源的复制，常常会造成复制品质量的下降，这反过来限制了使用复制品进行下一步复制的选择方案。随着向数字源的转换，复制的质量得以保证，保持复制品质量的一致已成为可能。[1291]

通过实施一些技术手段（数字版本管理或 DRM）来防止复制，娱乐行业已经对复制问题作出了响应，[1292] 但迄今为止，在它们被引入后不久，这些技术手段往往被违法者绕过。[1293] 国际互联网上涌现出各种各样可用的软件工具，使用户能够拷贝受 DRM 系统保护的音乐 CD 和电影 DVD。此外，国际互联网提供了不受限分发的机会。结果是，侵犯知识产权（尤其是版权）的行为是通过国际互联网广泛实施的一种违法行为。[1294]

《网络犯罪公约》：

因此，《公约》包括了一条涵盖这些版权侵权行为的条款，旨在协调国家法律中各种各样的规定：

[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.

[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.

第 10 条 — 与侵犯版权及相关权利有关的违法行为

（1）依据签约方根据 1971 年 7 月 24 日用于修订《关于文学和艺术作品保护的伯尔尼协定》的《巴黎法案》、《知识产权贸易相关问题协议》和《WIPO 版权条约》而需承担的义务（此类公约所规定的任何道德权利除外），当依据签约方法律而定义的版权侵权行为是有意、大规模并借助计算机系统手段进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为。

（2）依据签约方根据《保护表演者、音像作品制作者和广播组织的国际公约》（《罗马公约》）、《知识产权贸易相关问题协议》和《WIPO 表演和音像作品条约》而需承担的义务（此类公约所规定的任何道德权利除外），当依据签约方法律而定义的相关权利侵犯行为是有意、大规模并借助计算机系统手段进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为。

（3）假如有其他有效的补救措施可用、且此类保留无损本条款第 1 段和第 2 段中提及之国际文件中所述的签约方国际义务，那么在有限制的条件下，签约方可以保留权利，不施加本条款第 1 段和第 2 段下的刑事责任。

大多数国家已经对侵犯版权的行为进行定罪，[1295] 许多国际协定也已解决这一问题。[1296] 《公约》旨在提供一些基本的原则，来对侵犯版权的行为进行定罪，以便协调现有的国家法律。条款没有涵盖与专利或商标有关的侵权行为。[1297]

[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.
[...]
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.

参考国际协定：

与其他法律框架不同，《公约》并没有明确指定哪些行为将被定罪，而是参照了大量的国际协定。[1298] 这也是第 10 条备受批评的一个方面。这使得更难发现定罪的程度，而且这些协定可能在随后出现变更，除了这些事实，如果《公约》责成各签字国签署第 10 条中提到的国际协定，那么问题就出现了。《公约》的起草者指出，《网络犯罪公约》不得引入任何此类义务。[1299] 这样，那些尚未签署上述国际协定的国家，既不一定要签署协定，也不会被迫对与它们尚未签署的协定有关的犯罪行为进行定罪。因此，第 10 条仅仅对那些已经签署了上述协定的国家具有约束力。

心理因素：

由于其一般性，《公约》将定罪限定于那些借助计算机系统实施的违法行为。[1300] 除了通过计算机系统实施的犯罪行为之外，刑事责任也限定于那些故意实施的违法行为和大规模的违法行为。“故意”这一术语与《公约》其他实体法律条款中使用的“有意”这一术语是对应的，并且考虑到了《TRIPS 协定》第 61 条中 [1301] 使用的术语，该协定用于监管对版权侵犯行为进行定罪的义务。[1302]

大规模：

对违法行为须是大规模实施的这一限定，也考虑到了《与贸易有关的知识产权协定》（TRIPS），该协定要求刑事制裁只针对“大规模的盗版行为”。由于文件共享系统中的大多数版权

(e) As used in this section -
(1) the term“sphonorecord” 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.”

[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.

侵权行为并不是大规模实施的，因此，它们未被第 10 条所涵盖。《公约》寻求为与国际互联网有关的违法行为制定一些最低标准。因此，各方可以在对版权侵权犯罪定罪的过程中超越“大规模”这一界限。[1303]

未获授权：

一般地，由《网络犯罪公约》定义的实体刑法条款要求违法行为是“未获授权”而实施的。[1304]《公约》的起草者指出，“侵犯”这一术语已经暗示了该行为的实施是未获授权的。[1305]

限制与保留：

段落 3 使各签约国可以做出保留，只要有其他有效的补救措施可用，且所做保留无损各签约国的国际义务。

《斯坦福公约》草案：

非正式的[1306] 1999 年版的《斯坦福公约》草案没有包括对侵犯版权行为定罪的条款。《公约》起草者指出，版权犯罪之所以没有包含在内，是因为这可能已被证明困难的。[1307] 相反地，他们直接参考了现有的国际协定。[1308]

6.2 程序法

6.2.1 引言

正如上面各节所解释的那样，与网络犯罪作斗争，需要具备适当的实体刑法条款。[1309] 至少在大陆法系国家中，如果没有这些法律，那么执法机构将无法调查犯罪行为。但在与网络犯罪作斗争的过程中，执法机构的要求不限于实体刑法条款。[1310] 为了完成调查 — 除了培训和装备 — 它们还需

[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.

[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

要一些程序手段，使执法机构能够采取必要的措施来确定违法者并收集犯罪过程的证据。[1311] 这些措施可能与对那些与网络犯罪无关的犯罪进行调查所采取的措施是相同的 — 但鉴于以下事实，即违法者不必出现在犯罪现场，甚至不必接近犯罪现场，这就使得对网络犯罪的调查，很可能需要采取与传统犯罪调查不同的方式来进行。[1312]

之所以需要不同的调查方法，不仅仅是因为犯罪行为发生地和犯罪现场的独立性。在大多数情况下，正是上面提到的、执法机构所面临的众多挑战的结合，使得网络犯罪的调查显得很独特。[1313] 如果违法者在别的国家，[1314] 使用能够实现匿名通信的服务，此外，通过运用不同的公共互联网互联网终端来实施犯罪行为，那么对这种犯罪行为就很难仅仅通过诸如搜查和查封等传统的手段来进行调查了。为了避免误解，重要的是指出，对网络犯罪的调查既需要传统的侦查工作，也需要运用传统的调查手段 — 但网络犯罪调查还面临着一些无法仅通过传统调查手段就能解决的挑战。[1315]

有些国家已经采用了新的手段，使执法机构能够调查网络犯罪以及那些需要对计算机数据进行分析的传统犯罪。[1316] 在实体刑法方面是这种情况，《欧洲理事会关于网络犯罪的公约》包含一系列条款，反映了网络犯罪调查所需之程序手段方面的、被广泛接受的最低标准。[1317] 因此，此下内容将概述这一国际公约所提供的程序手段，此外还强调了一些该《公约》规定之外的国家方法。

6.2.2 计算机与国际互联网调查（计算机取证）

对“计算机取证”有多种多样的定义。[1318] 它可以定义为“对信息技术设备和系统进行检查，以便为刑事或民事调查获取信息”。[1319] 在实施犯罪时，嫌疑人会留下一些蛛丝马迹。[1320] 这种表述在传统犯罪调查和计算机犯罪调查中都是有效的。传统犯罪的调查与网络犯罪的调查之间主要的区

---

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.

[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.

别在以下事实，即网络犯罪调查一般需要一些与数据有关的特殊的调查技术，并且可以通过专用的软件工具来帮助调查。[1321] 除了适当的程序手段，进行此类分析还要求主管部门具备管理和分析相关数据的能力。取决于违法行为和涉及的计算机技术，在程序调查手段和取证分析技术方面的要求通常各不相同，[1322] 常常伴随着一些独特的挑战。[1323]

通常情况下，网络犯罪调查的这两个方面是密切相关的，而且通常用“计算机取证”这一专业术语或者是收集和分析证据来描述。[1324] 如上所述，“计算机取证”这一术语描述了运用计算机调查和分析技术来确定可能的证据。这包括众多方面的分析，从一般的分析，如在计算机硬盘上搜索儿童色情内容、[1325] 到特殊的调查，如 iPod 取证 [1326] 和访问加密的文件 [1327] 等。计算机取证方面的专家为专业警员和起诉人员进行的调查提供支持。在国际互联网调查中，举例来说，计算机取证专家可以在以下几方面提供所需的协助：[1328]

- 确定可能的数字踪迹（特别是确定通信流量数据可能的地点）；[1329]
- 支持国际互联网服务提供商确定他们能够提供的、用于支持调查的信息；
- 保护收集到的相关数据，并确保证据的连续性。[1330]

一旦确定了可能的证据，专家们还可以在以下方面提供援助，例如：

- 在分析期间保护有关的计算机系统上的数据不遭到更改或破坏；[1331]
- 在有关的计算机系统和存储介质上找到所有的相关文件；[1332]

[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.

[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

- 对加密的文件进行解密；[1333]
- 恢复被删除的文件；
- 如果有多人访问过该机器或设备，那么确定对计算机系统的使用情况；[1334]
- 揭示由应用程序和操作系统使用的临时文件的内容；
- 分析收集到的证据；[1335]
- 提供分析文件；[1336]
- 为进一步调查提供证据；
- 提供专家咨询和证词。

尤其是，取证专家参与保护证据的完整性，强调取证专家的工作与技术和法律两方面的结合。在这种背景下，一个主要的挑战是证据的连续性要求对原始数据准确的审核，以及要求取证专家开展大量的实际工作。[1337]

计算机取证专家可能的参与程度，显示了其在调查过程中的重要性。此外，成功的国际互联网调查对取证资源可用性的依赖，也突显了在这一领域进行培训的必要性。只有当调查人员或者在计算机取证方面接受过培训，或者能够接触这一领域的专家，才能够对网络犯罪开展有效的调查和起诉。

6.2.3 保护措施

在过去几年间，全世界的执法机构都强调了对适当调查手段的迫切需要。[1338] 考虑到这一点，《网络犯罪公约》在程序手段方面受到指责，也许会令人吃惊。[1339] 这种指责主要集中于以下方面，即《公约》包括了大量关于建立调查手段的规定（第 16 条至第 21 条），但只有一个条款（第 15 条）涉及了保护措施。[1340] 此外，还可以注意到，与《公约》中的实体刑法条款不同的是，在《公约》的执行过程中，几乎不存在各国进行调整的可能性。[1341] 这种指责本身主要集中于定量方面的问

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: 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.

题。《公约》遵循对保护措施实施集中管理而非将其分别依附于每一种手段的概念是正确的。但这并不一定意味着对嫌疑人权利的更弱保护。

《网络犯罪公约》最初是设计为一种与网络犯罪作斗争的国际框架和手段，而不仅限于欧洲理事会成员国。[1342] 在就必要的程序手段进行谈判的过程中，包括一些来自非欧洲国家（如美国和日本）代表在内的《公约》起草者认识到，涉及保护措施的现有国家方法、尤其是在各种不同刑法体系中保护犯罪嫌疑人的方式，都存在很大的差异，使得不可能为所有成员国提供一种详尽的解决方案。[1343] 因此，《公约》起草者决定不在《公约》的正文中包括特定的规则，而是要求各成员国确保在保护措施方面采用基本的国家标准和国际标准。[1344]

第 15 条 — 限制条件与保护措施

1．各方应确保，本节中所提之权力与程序的建立、执行和应用服从其本国法律中所提的限制条件与保护措施，这些限制条件与保护措施应提供适当的人权与自由保护，包括依据 1950 年版的《欧洲理事会关于保护人权和基本自由的公约》、1966 年版的《联合国关于民事和政治权利的国际协定》以及其他适用的国际人权规定下该签约方已承担之义务而提出的权利，这些限制条件与保护措施应结合均衡原则来考虑。

2．合适的话，考虑到有关程序或权力的特性以及其他相关问题，此类限制条件与保护措施应包括司法或其他独立的监督、理由的公正应用、以及有关此类权力或程序的范畴和时限的限制条件。

3．为了与公众利益保持一致，尤其是有效的司法监督，各方应考虑本节中所述之权力和程序对第三方权利、责任和合法权益的影响。

第 15 条基于以下原则：各签约国应采用根据其国内法律业已存在的限制条件与保护措施。如果法律提供了适用于所有调查手段的最主要标准，那么这些原则将适用于与国际互联网有关的手段。[1345] 如果国内法律不是基于有关保护措施与限制条件的集中规定，那么有必要对照与国际互联网有关的手段，来分析在传统手段方面所实施的保护措施与限制条件。

但《公约》不是单独参考国家法律中的现有保护措施。这可能带来一些不足，即采用的要求将在某种程度上不尽相同，使得法律协调的积极方面也不再适合。为确保那些可能拥有不同法律传统和保护措施的签约国能够执行某些标准，[1346] 通过参照基本的框架，《网络犯罪公约》定义了最低的标准，如下所述：

- 1950 年版的《欧洲理事会关于保护人权和基本自由的公约》；

[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 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.

- 1966年版的《联合国关于民事和政治权利的国际公约》；
- 其他适用的国际人权文件。

由于《公约》可以由不属于欧洲理事会成员国的国家签署和批准，[1347] 因此重要的是强调，在评估不属于《网络犯罪公约》成员国的签署国的保护措施系统时，不仅要考虑《联合国关于民事和政治权利的国际协定》，而且要考虑《欧洲理事会关于保护人权和基本自由的公约》。

至于网络犯罪调查，《网络犯罪公约》第15条中最相关的条款之一参照了《欧洲人权公约》第8条第2段的内容。

> **第8条**
>
> 1. 每个人都有权要求其私生活和家庭生活、住宅以及通信得到尊重。
>
> 2. 公共主管部门不得干预上述权利的行使，除非依照法律以及在民主社会中为了国家安全、公共安全或国家经济利益，为了防止混乱或犯罪，为了保护健康或道德，或者为了保护他人的权利和自由，有必要进行干预者，不在此限。

欧洲人权法院已经付出种种努力，力求更准确地定义用于管理电子调查、尤其是监视的标准。如今，判例法已经成为涉及与通信有关的调查方面最重要的国际标准之一。[1348] 判例法特别考虑了调查干预的严重性、[1349] 其目的 [1350] 以及其均衡性。[1351] 可从判例法中摘录的基本原则如下所述：

- 有必要为调查手段建立足够的法律基础；[1352]
- 法律基础在主题方面必须明晰；[1353]
- 执法机构的能力需要是可预测的；[1354]
- 对通信的监视只有在严重罪行的背景下才是合法的。[1355]

[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 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

除了这一点之外，《网络犯罪公约》第 15 条还考虑了均衡性原则。[1356] 该条款对那些非欧洲理事会成员国的签约国尤为相关。在这些情况下，现有的保护措施的国家体系没有适当地保护犯罪嫌疑人，强制性要求成员国在批准和实施过程中提出必要的保护措施。

最后，《网络犯罪公约》第 15 条第 2 小段明确提到了某些最相关的保护措施，[1357] 包括：

- 监管；
- 理由辩护应用；
- 在范围和持续期限方面的程序限制。

与上述基本原则不同，此处提到的这些保护措施并不一定需要得到执行，而是只有当从相关的特性或程序角度而言是合适的时候，才需执行。至于决定何时执行，则交由国家法律体系来决定。[1358]

与《网络犯罪公约》提供的保护措施系统有关的一个重要方面问题是，执法机构能否一方面灵活地使用这些手段，另一方面又能确保保护措施的有效性，而这取决于保护措施分级制度的实施。《公约》没有明确阻止各方对所有的手段实施相同的保护措施（如对法院命令的要求），但这样一种方法将影响到执法机构的灵活性。能否在保护措施的分级制度中确保对嫌疑人权利的适当保护，很大程度上取决于用相关的保护措施来平衡调查手段的潜在影响。为了实现这一点，有必要对低强度调查手段和高强度调查手段做区分。在《网络犯罪公约》中存在大量的、有关此类区分的例子，使各方能够进一步提出一种分级的保护体系。这些包括：

- 区分截获内容数据（第 21 条）[1359] 和收集通信流量数据（第 20 条）。[1360] 与收集通信流量数据不同，对内容数据进行截获仅限于严重犯罪。[1361]
- 区分命令快速保留所储存的计算机数据（第 16 条）[1362] 和根据提供数据命令提交所储存的计算机数据（第 18 条）。[1363] 第 16 条只能使执法机构命令保留好数据，而不能命令透露数据。[1364]
- 区分第 18 条中 [1365] 提交“订户信息”的义务[1366] 和提交“计算机数据”的义务。[1367]

---

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.

[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.

[1365] 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.

[1366] A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 Convention on Cybercrime.

[1367] A definition of the term "computer data" is provided in Art. 1 Convention on Cybercrime.

如果对调查手段的强度和对犯罪嫌疑人的潜在影响进行了正确评估，并根据分析的结果来设计保护措施，那么分级保护制度不会造成程序手段系统的不平衡。

6.2.4 加速保存与透露保存的计算机数据（快速冻结）

确定实施了网络犯罪的违法者常常需要对通信流量数据进行分析。[1368] 尤其是违法者使用的 IP 地址，将有助于执法机构对其实施跟踪。只要执法机构能够访问到相关的通信流量数据，那么在某些情况下，甚至可能确定一个在无需提供身份的公共国际互联网终端上实施犯罪的违法者。[1369]

调查者面临的主要困难之一是，与考虑中的信息高度相关的通信流量数据，常常在相当短的期限内就会被自动删除。这种自动删除的原因在于：在某一过程结束后（例如发送电子邮件、接入国际互联网完毕或下载电影），在过程当中产生的、确保这一过程得以完成的通信流量数据就不再需要。至于对这一动作的经济方面的考虑，大多数国际互联网提供商更愿意尽可能快地删除这些信息，原因是数据的保存时间越长，所需的存储容量将更大（更贵）。[1370]

不过，经济方面的问题并不是执法机构必须迅速完成其调查的唯一原因。有些国家有严格的法律，禁止在某一过程结束之后存储一定的通信流量数据。此类限制的一个例子是欧盟的《隐私与电子通信指令》第 6 条。[1371]

> **第 6 条 — 通信流量数据**
>
> 1. 公共通信提供商处理和存储与订户和用户有关的通信流量数据。
>
> 无损于本条第 2、3、5 段和第 15 条（1）的规定，当不再需要用于通信传输时，网络或公共电子通信服务必须被删除或者使之匿名。
>
> 2. 出于开具订户账单和互连支付的目的，可以对通信流量数据进行处理。但只有在账单合法异议或者费用支付期结束之前，才允许进行此类处理。

因此，时间是国际互联网调查的一个关键问题。通常情况下，很可能在作案、罪行被发现与执法机构发出通知之间已经过去了一些时间，因此重要的是要实施一些机制，防止相关数据在有时持续很长的调查过程中被删除。关于这一点，当前正在讨论两种不同的方法：[1372]

- 数据保留；以及
- 数据保存（“快速冻结程序”）。

[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.

[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.

数据保留义务迫使国际互联网服务提供商在一定期限内保存通信流量数据。[1373] 在最新的法律方法中，记录需要保存 6 到 24 个月。[1374] 这将使执法机构甚至能够在案发后数月内访问到用于确定违法者所需的数据。[1375] 欧盟议会最近批准了数据保留义务，[1376] 美国当前也正在讨论这一方法。[1377] 关于数据保留的原则，可以在以下找到更多的信息。

《网络犯罪公约》：

数据保存是确保网络犯罪调查不至于仅仅因为在长时间持续的调查过程中因通信流量数据被删除而失败的另一种不同方法。[1378] 根据有关数据保存的法律，执法机构可以命令服务提供商防止某些数据被删除。加速保存计算机数据是一种能够使执法机构立即做出响应并避免数据因长时间调查程序而被删除的风险的手段。[1379] 《网络犯罪公约》的起草者决定将重点放在“数据保存”而非“数据保留”。[1380] 在《网络犯罪公约》第 16 条中可发现一条有关的规定。

> **第 16 条 — 加速保存所储存的计算机数据**
>
> 1．各方应采取必要的法律措施和其他措施，以使具有法定资格的主管部门能够通过命令或类似方式获得加速保存的特定的计算机数据，包括通过计算机系统手段已经储存的通信流量数据，尤其是在存在认为计算机数据极易丢失或被修改的依据的情况下。
>
> 2．当签约方通过命令形式要求某人保存其所有或控制的、特定的计算机数据以实现上述第 1 段的目的时，签约方应采取必要的法律措施和其他措施，责成该人在不超过 90 天的必要时间期限内，保存和维护好这些计算机数据的完整性，以使具有法定资格的主管部门能够寻求将其公开的权力。签约方可以提供这样的一个命令，以便后续更新。

[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.

3．各方应采取必要的法律措施和其他措施，责成将要执行计算机数据保存任务的管理人或其他人，在签约方的国内法律规定的一段时间内，对此类程序的执行情况保守秘密。

4．本条款中提及的权力和程序应服从第 14 条和第 15 条。

从国际互联网服务提供商的角度来看，相比数据保留，数据保存是一种强度较弱的手段。[1381] 国际互联网服务提供商不需要为所有用户保存所有数据，但相反地，一旦它们收到有关主管部门的命令，必须确保特定的数据不会被删除。数据保存提供了一些优势，原因是它不仅涵盖了从提供商角度来看的数据保存，还涵盖了从数据保护角度来看的数据保存。并不一定要保存来自数百万国际互联网用户的数据，而只需保存那些在犯罪调查中与可能的嫌疑人有关的数据。尽管如此，重要的是指出，在违法行为结束后数据可能被立刻删除的情形中，数据保留是有优势的。在这些情况下，数据保存命令将 — 不同于数据保留义务 — 无法阻止对相关数据的删除。

依照第 16 条发出的命令，仅责成提供商保存它所处理的数据并在接到命令的时候不被删除。[1382] 这不限于通信流量数据，原因是通信流量数据只是作为一个例子而提及。第 16 条没有强迫提供商开始收集它们通常不会保存的信息。[1383] 此外，第 16 条没有责成提供商将相关的数据传输给主管部门。这一条款只是授权执法机构防止删除相关数据，而不是要提供商允诺传输数据。在《网络犯罪公约》第 17 条和第 18 条中对数据传输义务做了规定。将保存数据的义务与透露数据的义务分开，其优点体现在以下事实，即有可能为其应用要求不同的条件。[1384] 至于快速反应的重要性，举例来说，它将支持通过法官的命令来放弃要求，并使起诉能够进行或者使警察能够命令保存数据。[1385] 这将使主管部门能够更加迅速地做出反应。可以通过要求一个透露数据的命令，来实现对嫌疑人权利的保护。[1386]

透露所保存的数据是《网络犯罪公约》第 18 条中规定的其他方面问题：

第 18 条 — 提供数据命令

1．各方应采取必要的法律措施和其他措施，以使具有法定资格的主管部门能够命令：

a. 该签约方管辖范围内的人提交其所有或控制的、特定的计算机数据，数据储存于计算机系统或计算机数据存储介质中；以及

[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 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."

b. 在该签约方管辖范围内提供服务的服务提供商提交该服务提供商所有或控制的、与此类服务有关的订户信息。

2．本条款中提及的权力与程序应服从第 14 条和第 15 条。

3．出于本条款的目的，术语“订户信息”是指以计算机数据形式或任何其他形式包含的、由服务提供商持有的任何信息，这些信息与该服务的订户有关，而非通信流量数据或内容数据，通过这些信息可以确定：

a. 使用的通讯服务的类型、其采用的技术规定和服务的期限；

b. 依据服务协议或安排可获得的、有关订户身份、邮政地址或地理地址、电话和其他接入号码、账单和支付情况的信息；

c. 依据服务协议或安排可获得的、有关通信设备安装站点的任何其他信息。

根据《网络犯罪公约》第 18 条第 1 a）小节，可责成已保存了数据的提供商透露数据。

《网络犯罪公约》第 18 条不只是在遵照《网络犯罪公约》第 16 条发出保存命令后适用。[1387] 这一条款是执法机构可以利用的一种普通手段。如果**提供数据命令的接收者**自愿传输要求的数据，那么执法机构不**限于**查封硬件，还可以运用不太强硬的提供数据命令。相比真正的查封硬件，提交相关信息的命令通常不太强硬。因此，在那些取证调查不一定要求访问硬件的案件中，尤其可以运用这种命令。

除了提交计算机数据的义务之外，《网络犯罪公约》第 18 条还使执法机构能够命令提供订户信息。这一调查手段来自于基于 IP 调查的极端重要性。如果执法机构能够确定违法者在实施犯罪时使用的 IP 地址，那么它们将需要确定在犯罪发生之时使用该 IP 地址的人。[1388] 根据《网络犯罪公约》第 18 条第 1 b）小节，责成提供商提供第 18 条第 3 小节中所列的那些订户信息。[1389]

在执法机构逆路由追踪违法者并且需要立即访问以确定通信传输路径的那些情形中，第 17 条使它们能够命令快速部分透露通信流量数据。

第 17 条 — 加速保存和部分公开通信流量数据

1．关于依据第 16 条要保存的通信流量数据，各方应采取必要的法律措施和其他措施，以便：

a. 确保通信流量数据的这种快速保存是可以实现的，而不论该通信的传输过程是涉及一个还是多个服务提供商；以及

b. 确保向签约方具有法定资格的主管部门或者该主管部门指定的人快速透露足够量的通信流量数据，以使签约方能够确定服务提供商和通信传输途径。

[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 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).

2．本条款中提及的权力和程序应服从第 14 条和第 15 条。

如上所述，《公约》严格区分要求的保存数据义务与向具有法定资格的主管部门透露数据的义务。[1390] 第 17 条提供了明确的分类，原因是它将确保在涉及众多服务提供商的情形中保存通信流量数据的义务与透露必要的信息以确定路径的义务结合起来了。没有这种部分透露，在某些情况下，如果涉及多个提供商，那么执法机构将无法追踪违法者。[1391] 由于这两种义务的结合以不同的方式影响到了嫌疑人的权利，因此有必要重点讨论与这一手段有关的保护措施。

《英联邦计算机以及与计算机有关的犯罪的示范法》：

在 2002 年版的《英联邦示范法》中可以找到类似的方法。[1392]

条款：

第 15 节

如果地方法官对警察运用规定的计算机数据或者打印资料或其他信息确信其必要性，认为它是出于犯罪调查或犯罪审理目的而合理要求的，那么地方法官可以命令：

（a）在[制定法律国家]管辖范围内、控制计算机系统的人，从系统规定的计算机数据、打印资料或者这种数据的其他可理解的输出中提供数据；以及

（b）在[制定法律国家]管辖范围内的国际互联网服务提供商提供关于服务订户或以其他方式使用了该服务的用户的信息；以及

（c）[1393] 在[制定法律国家]管辖范围内、能够访问规定的计算机系统的人，从系统中处理并汇编好规定的计算机数据，并将其提交给规定的人员。

第 16 节 [1394]

如果警官确信保存在计算机系统中数据的必要性，出于调查犯罪的目的合理地要求提供，那么警官可以通过书面的形式通知控制该计算机系统的人，要求该人透露关于某一特定通信的足够的通信流量数据，以确定：

（a）服务提供商；以及

[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.

[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.

（b）通信传输的路径。

第 17 节

（1）如果警官确信

（a）保存在计算机系统中数据的必要性，出于调查犯罪的目的合理地要求提供；并且

（b）该数据存在可能被破坏或使之无法再被访问的风险；

那么警官可以通过书面的形式，通知控制该计算机系统的人，要求他确保通知中规定的数据保存一段通知中规定的时间（最多 7 天）。

（2）如果是单方面应用，[法官][地方法官]授权延长规定的时间，那么这一期限可以延长，可以超过 7 天。

6.2.5 数据保留

数据保留义务迫使国际互联网服务提供商在一定期限内保存通信流量数据。[1395] 履行数据保留义务是在数据被删除之前避免出现上面所述难以访问通信流量数据之问题的一种方法。《欧盟关于数据保留的指令》是这种方法的一个例子。[1396]

第 3 条 — 保留数据的义务

1. 为了部分废除《指令 2002/58/EC》第 5、6 和 9 条，各成员国应采取措施确保本《指令》第 5 条中规定的数据依照其中的条款得以保留，在这个意义上，这些数据是由公共可用的电子通信服务提供商或公共通信网络提供商，在其提供相应通信服务的过程中、在其管辖范围内产生和处理的。

2. 保留第 1 段中所规定之数据的义务应包括保留第 5 条中所规定的数据，它们涉及不成功的呼叫尝试，其中，这些数据是由公共可用的电子通信服务提供商或公共通信网络提供上，在其提供相应通信服务的过程中、在相关成员国的管辖范围内产生或处理以及保存（对于电话数据）或记录（对于国际互联网数据）的。本《指令》不得要求保留与未连接呼叫有关的数据。

第 4 条 — 访问数据

各成员国应采取措施，确保根据本《指令》保留的数据只在特殊情况下提供给具有法定资格的国家主管部门，并且依照国家法律进行提供。为了依照必要性和均衡性要求访问已保留的数据，要遵守的程序以及需满足的条件应由各成员国在其国家法律中确定，并遵守欧盟法律或公共的国际法律的相关规定，尤其是由欧洲人权法院解释的 ECHR。

[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.

第 5 条 — 要保留的数据类别

1．各成员国须确保以下类别的数据根据本《指令》得以保留：

（a）用于跟踪和确定通信源而所需的数据：

（1）涉及固定网络电话和移动电话；

（i） 呼叫的电话号码；

（ii）订户或注册用户的姓名和地址；

（2）涉及国际互联网接入、国际互联网电子邮件和国际互联网电话：

（i） 分配的用户 ID 号；

（ii）为任何进入公共电话网络的通信分配的用户 ID 号和电话号码；

（iii）订户或注册用户的姓名和地址以及在通信时分配的国际互联网协议（IP）地址、用户 ID 号或电话号码；

（b）用于确定通信目的地而所需的数据；

（1）涉及固定网络电话和移动电话：

（i） 拨叫的号码（被叫的电话号码），以及在涉及如呼叫转移或呼叫转接等辅助业务的情况下，呼叫被路由的单个或多个号码；

（ii）订户或注册用户的姓名和地址；

（2）涉及国际互联网电子邮件和国际互联网电话：

（i） 用户 ID 号或国际互联网电话预期接听者的电话号码；

（ii）订户或注册用户的姓名和地址，以及通话预期接听者的用户 ID 号；

（c）用于确定通信日期、时间和持续时间而所需的数据：

（1）涉及固定网络电话和移动电话的通信起始日期与时间以及终止日期与时间；

（2）涉及国际互联网接入、国际互联网电子邮件和国际互联网电话：

（i） 根据特定的时区登录和退出国际互联网接入服务的日期与时间，加上由国际互联网接入服务提供商为通信而分配的 IP 地址，不管它是动态的还是静态的，以及订户或注册用户的用户 ID 号；

（ii）根据特定的时区登录和退出国际互联网电子邮件服务或国际互联网电话服务的日期和时间；

（d）用于确定通信类型而所需的数据：

（1）涉及固定网络电话和移动电话：使用的电话服务；

（2）涉及国际互联网电子邮件和国际互联网电话：使用的国际互联网服务；

(e) 用于确定用户通信设备或者声称是其设备而所需的数据:

(1) 涉及固定网络电话、主叫和被叫电话号码;

(2) 涉及移动电话:

(i) 主叫和被叫电话号码;

(ii) 呼叫方的国际移动用户标识（IMSI）;

(iii) 呼叫方的国际移动设备标识（IMEI）;

(iv) 被叫方的 IMSI;

(v) 被叫方的 IMEI;

(vi) 在预付费的匿名服务中，服务最初激活的日期和时间以及服务被激活的位置标签（单元 ID 号）;

(3) 涉及国际互联网接入、国际互联网电子邮件和国际互联网电话:

(i) 拨号上网的主叫电话号码;

(ii) 数字用户线路（DSL）或通信发起者的其他端点;

(f) 用于确定移动通信设备位置而所需的数据:

(1) 通信开始时的位置标签（单元 ID 号）;

(2) 通过参考通信流量数据保留期间的位置标签（单元 ID 号）来确定单元地理位置的数据。

2. 依据本《指令》，不得保留任何揭示通信内容的数据。

第 6 条 — 保留期限

各成员国应确保第 5 条中所规定的数据类别保留期限不小于 6 个月但不超过 2 年，保留日期从通信日期开始起算。

第 7 条 — 数据保护与数据安全

无损于依照《指令 95/46/EC》和《指令 2002/58/EC》而批准的条款，各成员国应确保公共可用的电子通信服务或公共通信网络的提供商，至少尊重以下依据本《指令》的、有关数据保留的数据安全性原则:

(a) 保留的数据应具备与网络上的那些数据相同的质量，并服从同样的安全与保护原则;

(b) 数据应服从适当的技术和组织措施，以保护数据免受意外或非法的破坏、意外的损失或更改，或者未获授权或非法的保存、处理、访问或透露;

(c) 数据应服从适当的技术和组织措施，以确保它们只能由特殊授权人员访问；以及

(d) 那些已被访问和保存的数据除外，数据应在保留期限的最后予以销毁。

第 8 条 – 已保留数据的存储要求

各成员国应确保以以下方式、依据本《指令》来保留第 5 条中所规定的数据，即一旦要求，能够向具有法定资格的主管部门传输所保留的数据以及任何其他相关信息，而不造成过度延迟。

以下事实，即《指令》将涵盖有关国际互联网任何通信的重要信息，遭到了人权组织的猛烈批评。[1397] 这种批评反过来可能导致宪法法院对《指令》及其执行情况进行评审。[1398] 此外，在其对 In Productores de Música de España（Promusicae）v. Telefónica de España [1399] 案件的评论中，欧洲法院法律总顾问 Juliane Kokott 女士指出，数据保留义务能否在不违犯基本权利的情况下执行值得怀疑。[1400] 至于执行此类规定方面存在的困难，已 2001 年的八国集团峰会上指出。[1401]

但批评不只限于这一方面。数据保留在与网络犯罪作斗争过程中变得不太有效的另一个原因在以下事实，即这一义务可被绕过。躲避数据保留义务的最简单方法包括：

- 使用不同的公共国际互联网终端或者无需注册的预付费的手机数据服务，以及 [1402]
- 在不存在数据保留义务的国家中使用匿名通信服务（至少是部分地使用）。[1403]

如果违法者使用不同的公共终端或者无需注册、由提供商保存数据的预付费手机数据服务，那么数据保留义务只可能使执法机构找到服务提供商，而无法找到真正的违法者。[1404]

除此之外，违法者还可通过使用匿名通信服务器来躲避数据保留义务。[1405] 在这种情况下，执法机构也许能够证明违法者和使用的匿名通信服务器，但由于无法访问到匿名通信服务器所在国家的通信流量数据，因此可能无法证明违法者参与了某一犯罪行为。[1406]

[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.

[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.

至于非常容易躲避这一条款的事实，在欧盟，履行数据保留义务还伴随着一种担心，即其履行过程还将要求一些必要的辅助措施，以确保手段的有效性。可能的辅助措施可以包括要求在使用在线服务之前先进行注册，[1407] 或者禁止使用匿名通信技术。[1408]

6.2.6 搜查与查封

尽管有些国家正在讨论并已经采用了一些新的调查手段，比如实时收集内容数据、使用远程取证软件来确定违法者等，但搜索与查封仍然是最重要的调查手段之一。[1409] 只要确定了违法者，执法机构就可以查封其信息技术设备，而计算机取证专家可以对该设备进行分析，以收集起诉所需的证据。[1410]

在一些欧洲国家和美国，当前正在讨论替换或修改搜索与查封程序的可能性。[1411] 一种无需进入嫌疑人住所搜查和查封计算机设备的可能性将是执行在线搜索。这种手段将在以下章节中做更详细描述，它指的是执法机构通过国际互联网访问嫌疑人的计算机以执行秘密搜索程序的一种方法。[1412] 尽管执法机构可能明显受益于以下事实，即调查可以在嫌疑人不察觉的情况下进行，对硬件的物理访问是一种更加有效的调查技术。[1413] 这突显了在国际互联网调查中搜索与查封程序的重要作用。

《网络犯罪公约》：

大多数国家的刑事程序法包含了使执法机构能够实现搜索与查封目标的条款。[1414] 《网络犯罪公约》的起草者绝不会忽略搜索与查封程序，其中一个原因在于国家法律通常不会包含与数据有关的搜索与查封程序。[1415] 比如，有些国家将搜索与查封程序的应用限定在查封具体的物品。[1416] 基于此类规定，法律调查人员能够查封整个服务器，但不能做到通过从服务器中复制相关数据而仅仅查

[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.

[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.

封相关数据。如果相关的信息保存在某个服务器上，而该服务器上存着数百位其他用户的数据，那么当执法机构查封该服务器后，其他用户将也无法再使用，在这种情况下，查封整个服务器将带来困难。另一个例子是，当传统的搜查和查封有形物品的方法不够用时，如执法机构不知道服务器的具体位置，但能够通过国际互联网访问到它。[1417]

《网络犯罪公约》第 19 条第 1 小段着眼于建立一种能够对计算机系统进行搜索的手段，这种手段与传统的搜索程序一样有效。[1418]

第 19 条 – 搜查和查封储存的计算机数据

1．各方应采取必要的法律措施和其他措施，以使具有法定资格的主管部门能够进行搜查或做类似访问：

a. 计算机系统或其组成部分以及储存在其中的计算机数据；以及

b. 计算机数据可以储存在其中的计算机数据存储介质。

尽管搜查和查封程序是调查人员常用的一种手段，但在网络犯罪调查中，它的应用将存在诸多挑战。[1419] 其中一个主要困难是搜查命令常常限于某些地点（如犯罪嫌疑人的家）。[1420] 至于搜查计算机数据，在调查期间有可能发现，嫌疑人没有将它们存储在本地的硬盘驱动器上，而是存储在他通过国际互联网进行访问的外部服务器上。[1421] 使用国际互联网服务器来存储数据和处理数据，在国际互联网用户中正变得日益流行（“云计算”）。在国际互联网服务器上存储信息的优点之一是，可以在任何有国际互联网连接的地方访问到这些信息。为了确保调查的有效进行，重要的是保持调查的某种灵活性。如果调查人员发现相关的信息存储在另一个计算机系统中，那么他们应当能够延伸对这一系统的搜查。[1422] 《网络犯罪公约》在第 19 条第 2 小段中解决了这一问题。

第 19 条 – 搜查和查封储存的计算机数据

[…]

2．各方应采取必要的法律措施和其他措施，以确保在其主管部门依照第 1a 段搜查或类似地访问特定的计算机系统或其一部分、并有依据认为搜查的数据储存在签约方管辖范

[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.

[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.

围内的另一个计算机系统或其一部分内、以及对最初系统而言此类数据的进出为合法的情况下，该主管部门应能够迅速扩大对其他系统的搜查或类似地访问。

另一个挑战涉及查封计算机数据。如果调查人员决定，没有必要查封用来存储信息的硬件，或者这样认为做不恰当，他们仍然需要其他手段来使自己能够继续对所存储计算机数据的搜查和查封程序。[1423] 必要的手段不限于拷贝相关数据的行为。[1424] 此外，还有大量的辅助措施是维持要求的效率所必需的，如查封计算机系统本身。最重要的问题是保持所拷贝数据的完整性。[1425] 如果调查人员不具备采取必要的措施以确保所拷贝数据完整性的许可，那么拷贝的数据可能不会在刑事起诉过程中作为证据被接受。[1426] 在调查人员拷贝了数据并采取措施保持数据完整性后，他们需要决定怎样处置原始数据。由于调查人员不会在查封过程中拆除硬件，因此信息一般还会在原地。尤其是涉及非法内容 [1427]（如儿童色情）的调查，调查人员不能将数据留在服务器上。因此，他们需要一种手段使自己能够移去数据，或者至少确保这些数据不再被访问到。[1428] 《网络犯罪公约》在第 19 条第 3 小段中解决了上述问题。

第 19 条 — 搜查和查封储存的计算机数据

[…]

3．各方应采取必要的法律措施和其他措施，以使具有法定资格的主管部门能够查封或类似地保证能够依据第 1 条或第 2 条访问计算机数据。这些措施应包括以下权力：

a. 查封或类似地取得计算机系统或其一部分或计算机数据存储介质；

b. 制作和保留一份这些计算机数据的副本；

c. 维护相关的储存之计算机数据的完整性；

d. 致使所访问计算机系统中的那些计算机数据不可访问或移走。

[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.

[1428] One possibility to prevent access to the information without deleting them is the use encryption technology.

涉及计算机数据搜索命令的一个更大挑战在于，有时执法机构难以找到数据的位置。它们常常存储在特定国家管辖范围之外的计算机系统中。即使知道了确切位置，所存储数据的数量通常也会阻碍调查的加速进行。[1429] 在这些情况下，调查面临一些特殊的困难，原因是这些犯罪具有国际性，需要在调查过程中得到国际合作。[1430] 即使当调查涉及到国境之内的计算机系统，且调查人员已确定运营服务器的托管服务提供商，违法者将相关数据保存在了这些服务器上，调查人员也可能在确定数据的准确位置方面面临困难。甚至中小规模的托管服务提供商，也可能拥有数百台服务器和数千个硬盘，这完全有可能。更多情况下，在负责服务器基础设施的系统管理员的帮助下，调查人员无法确定准确的位置。[1431] 即使他们能够确定特定的硬盘驱动器，保护措施也可能阻止他们搜索相关的数据。《公约》的起草者决定通过执行一种强制性措施来解决这一问题，以促进对计算机数据的搜查与查封。第 19 条第 4 小段使调查人员能够迫使系统管理员为执法机构提供协助。尽管遵守调查人员命令的义务仅限于案件所需的信息和支持，但这一手段改变了搜查和查封程序的特性。在许多国家，搜查和查封命令只能迫使接受调查的人们容忍调查的过程 — 他们不必为调查提供主动支持。至于调查人员所需的具有专业知识的人员，《网络犯罪公约》的实施将以两种方式来改变这一状况。首先，他们需要提供调查人员所需的信息。第二种改变涉及到这一义务。为调查人员提供 — 合理 — 支持的义务，将使受到合约义务的约束或由监管者命令而工作的、具有专业知识的人员解放出来。[1432] 《公约》没有定义“合理”这一术语，但《解释报告》指出，“合理”“可能包括向调查主管部门透露密码或其他保护措施”，但一般不包括伴随“对其他用户的隐私或未授权搜索的其他数据构成不合理威胁”的透露密码或其他保护措施。[1433]

第 19 条 — 搜查和查封储存的计算机数据

[…]

4．各方应采取必要的法律措施和其他措施，以使具有法定资格的主管部门能够命令了解计算机系统功能运作或应用措施的任何人，保护好此处所指的、能够提供合理和必要信息的计算机数据，以确保第 1 段和第 2 段中所提及的措施得以实施。

[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.

[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.

《英联邦计算机以及与计算机有关的犯罪的示范法》：

在 2002 年版的《英联邦示范法》中可以找到一种类似的方法。[1434]

第 11 节

在这部分中：

[...]

“查封”包括：

（a）制作和保留计算机数据的副本，包括通过使用现场设备；以及

（b）使被访问计算机中的计算机数据不可访问或移去这些计算机数据；以及

（c）获得计算机数据输出结果的打印资料。

第 12 节 [1435]

（2）如果地方法官对[法院上宣过誓的][书面陈述的][信息]确信其必要性，对[嫌疑人]合理推断，认为存在某物或计算机数据：

（a）可能是证明违法行为的物证；或者

（b）是因某种违法行为的结果而由某人获取的；

那么地方法官[可][应]发出许可证，授权[执法结构][警官]，在必要的协助下，进入该处，搜查和查封该物或计算机数据。

第 13 节 [1436]

（1）拥有或控制某个计算机数据存储介质或计算机系统的人，依据第 12 节即搜查的对象，必须允许并在必要时协助搜查人员：

（a）访问和使用计算机系统或计算机数据存储介质，以搜查任何可用的或保存在系统中的计算机数据；以及

（b）获取和拷贝该计算机数据；以及

（c）使用设备来拷贝；以及

（d）获取一种来自计算机系统的可理解的输出，以人们可阅读的普通文本格式。

[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.*

（2）当没有合法或正当理由，某人未允许或协助他人实施可惩罚的违法行为时，在定罪时，处以不超过[一定期限]的监禁，或者不超过[一定数量]的罚款，或者两项并罚。

6.2.7 提供数据命令

即使某项义务在国内法律中没有得到执行，比如在《网络犯罪公约》第 19 条第 4 小段中的义务，提供商通常也与执法机构合作，以避免对其业务产生负面影响。如果 — 由于未得到提供商的合作 — 调查人员不能找到他们需要搜查和查封的数据或存储设备，那么调查人员可能需要查封更多的、超过通常所需的硬件设备。因此，一般地，提供商会为调查提供支持，并根据执法机构的要求提供相关的数据。如果拥有相关数据的人员向调查人员提交了它们，那么《网络犯罪公约》包含一些使调查人员能够放弃搜查命令的手段。[1437]

尽管执法机构与服务提供商共同努力，甚至在不存在法律基础的情况下，两者似乎建立了积极的公私关系，但仍存在许多与非规定之合作有关的困难。除了数据保护问题之外，主要的担心在于，如果服务提供商没有充分的法律依据而根据请求向调查人员提交了某些数据，那么他们可能违反了与客户的合约义务。[1438]

第 18 条 — 提供数据命令

1．各方应采取必要的法律措施和其他措施，以使具有法定资格的主管部门能够命令：

a. 该签约方管辖范围内的人提交其所有或控制的、特定的计算机数据，数据储存于计算机系统或计算机数据存储介质中；以及

b. 在该签约方管辖范围内提供服务的服务提供商提交该服务提供商所有或控制的、与此类服务有关的订户信息。

第 18 条包含两项义务。根据第 18 条第 1a）小段，任何人（包括服务提供商）有义务提交规定的、某人拥有或控制的计算机数据。与第 1b）小段不同，该条款的应用不限于特定数据。“拥有”这一术语要求该人物理访问了存储有特定信息的数据存储设备。[1439] “控制”这一术语进一步延伸了条款的应用。即使他没有物理访问，但正管理着该信息，那么认为该信息就处于他的控制下。例如，如果犯罪嫌疑人在远程在线存储系统中保存着相关的数据，那么就属于这种情况。尽管这样，在《解释报告》中，《公约》的起草者指出，单纯的、从技术角度能够远程访问存储的数据，并不一定形成控制。[1440] 因此，《网络犯罪公约》第 18 条的应用仅限于以下情形，即犯罪嫌疑人的控制程度已超出可能访问它们的可能性。

[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.
[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.

第 1b）小段包含一种仅限于某些数据的提供数据命令。根据第 18 条第 1b）小段，调查人员可以命令服务提供商提交订户信息。订户信息是确定违法者必备的要素。如果调查人员能够发现违法者使用的 IP 地址，那么他们需要将这一号码与某一个人联系起来。[1441] 在大多数情况下，IP 地址仅指向向用户提供 IP 地址的国际互联网提供商。在能够使用某项服务之前，国际互联网提供商通常要求用户用其订户信息进行注册。[1442] 在这一背景下，重要的是强调，《网络犯罪公约》第 18 条既不会执行数据保留义务，[1443] 也不会执行服务提供商注册订户信息的义务。[1444] 第 18 条第 1b）小段允许调查人员命令提供商提交这种订户信息。

初看起来，区分第 1a）小段中的“计算机数据”与第 1b）小段中的“订户信息”似乎没有必要，原因是第 1a）小段也涵盖以数字格式保存的订户信息。要进行区分的第一个原因涉及“计算机数据”与“订户信息”的不同定义。与“计算机数据”不同，“订户信息”这一术语不要求信息作为计算机数据保存。《网络犯罪公约》第 18 条第 1b）小段使得具有法定资格的法律主管部门能够提交以非数字格式保存的信息。[1445]

第 1 条 – 定义

2．出于本《公约》的目的：

b. “计算机数据”是指以某种适于在计算机系统中进行处理的形式表示的事实、信息或概念，包括适于促使计算机系统行使某种功能的程序；

第 18 条 – 提供数据命令

3．出于本条款的目的，术语“订户信息”是指以计算机数据形式或任何其他形式包含的、由服务提供商持有的任何信息，这些信息与该服务的订户有关，而非通信流量数据或内容数据，通过这些信息可以确定：

a. 使用的通信服务的类型、其采用的技术规定和服务的期限；

b. 依据服务协议或安排可获得的、有关订户身份、邮政地址或地理地址、电话和其他接入号码、账单和支付情况的信息；

c. 依据服务协议或安排可获得的、有关通信设备安装站点的任何其他信息。

[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.

区分“计算机数据”与“订户信息”的第二个原因是，它使立法者能够对各种手段的运用执行不同的要求。[1446] 比如，对于与第 1b）小段有关的提供数据命令，有可能执行更严格的要求，[1447] 原因是这一手段允许执法机构访问任何种类的计算机数据，包括内容数据。[1448] 实时收集通信流量数据（第 20 条）[1449] 和实时收集内容数据（第 21 条）[1450] 之间的区分表明，《公约》的起草者认识到，取决于讨论中的数据种类，执法机构可以访问需要得到执行的不同的保护措施。[1451] 有了“计算机数据”与“订户信息”的区分，《网络犯罪公约》第 18 条使各签约国能够在提供数据命令方面提出一个类似的分级保护体系。[1452]

《英联邦计算机以及与计算机有关的犯罪的示范法》

在 2002 年版的《英联邦示范法》中可以找到一种类似的方法。[1453]

> **第 15 节**
>
> 如果地方法官对警察运用规定的计算机数据或者打印资料或其他信息确信其必要性，认为它是出于犯罪调查或犯罪审理目的而合理要求的，那么地方法官可以命令：
>
> (a) 在[制定法律国家]管辖范围内、控制计算机系统的人，从系统规定的计算机数据、打印资料或者这种数据的其他可理解的输出中提供数据；以及
>
> (b) 在[制定法律国家]管辖范围内的国际互联网服务提供商提供关于服务订户或以其他方式使用了该服务的用户的信息；以及

[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.

（c）[1454] 在[制定法律国家]管辖范围内、能够访问规定的计算机系统的人，从系统中处理并汇编好规定的计算机数据，并将其提交给规定的人员。

6.2.8 实时收集数据

在许多国家中，电话监控是一种用于死罪调查的手段。[1455] 许多涉及使用电话的违法行为 — 尤其是移动电话 — 或者是在准备阶段，或者是在违法行为的实施阶段。特别是在涉及毒品买卖的案件中，对作案者之间的电话通话进行监控，可能是成功调查的关键所在。这一手段使调查者能够收集到宝贵的信息，尽管它限于在所监控线路/电话上交换的信息。如果违法者使用其他交换手段（如信件）或者没有处于监控的电话线路，那么调查人员将无法记录谈话内容。如果作案者之间不使用电话而直接见面交谈，那么通常也是这种情况。[1456]

如今，数据的交换已经取代了传统的电话交谈。数据交换不仅限于电子邮件和文件传输。通过使用基于国际互联网协议的技术（经由 IP 的话音）而进行的语音交谈，正日益增多。[1457] 从技术角度来看，IP 语音电话（VoIP）比起电子邮件交换以及使用电话线路的传统电话更先进，原因是截获这类电话的内容存在许多独特的困难。[1458]

随着大量的计算机犯罪涉及到数据交换，能够同样地拦截这些过程，或者以其他方式使用涉及交换过程的数据，可能成为成功调查网络犯罪的关键因素。在网络犯罪调查中，现有电话监控条款以及与使用电信流量数据有关的条款的应用，在某些国家已变得很难。遇到的困难既涉及技术问题，[1459] 也涉及法律问题。从法律角度来看，授权对电话交谈进行录音，并不一定包括授权对数据传输过程进行截获。

《网络犯罪公约》旨在缩小执法机构在监控数据传输过程的能力上现有的差距。[1460] 在这种方法中，《网络犯罪公约》区分了数据传输监控的两个子集。第 20 条授权调查人员收集通信流量数据。在《网络犯罪公约》第 1 条 d）中对“通信流量数据”这一术语进行了定义。

[1454] 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.*

[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.

第 1 条 — 定义

d. “通信流量数据”是指任何与借助计算机系统手段进行的通信有关的计算机数据，该数据由构成通信链的一部分的计算机系统生成，指明了通信的来源、目的地、路径、时间、日期、大小、持续时间或基本服务类型。

“内容数据”与“通信流量数据”之间的差别，与大多数相关国家法律中所用的区分标准是相同的。[1461]

6.2.9 收集通信流量数据

《网络犯罪公约》：

至于各国之间对通信流量数据的定义各不相同这一事实，[1462] 《网络犯罪公约》的起草者决定定义这一术语，以便在国际调查中改进对相关条款的应用。“通信流量数据”这一术语用于描述在通信过程中产生的、旨在将通信从其源头路由至其目的地的数据。无论何时只要用户连接到国际互联网，下载电子邮件或打开网站，就会产生通信流量数据。至于网络犯罪调查，源头和目的地涉及的通信流量数据中，最为相关的是 IP 地址，它可确定与国际互联网有关的通信中的通信参与者。[1463]

与“内容数据”不同，术语“通信流量数据”仅仅涵盖在数据传输过程中产生的数据，而不涵盖所传输的数据本身。尽管在某些情况下，访问内容数据也许是必要的，原因是它使执法机构能够以一种有效得多的方式来对通信进行分析。[1464] 虽然访问内容数据能使执法机构分析所交换文件的消息特性，但通信流量数据是确定违法者的必备数据。比如，在儿童色情案件中，通信流量数据使调查人员能够确定违法者向其上载儿童色情图像的网页。通过监控在使用国际互联网服务中产生的通信流量数据，执法机构能够确定服务器的 IP 地址，并随后可以试图确定其所在的物理位置。

第 20 条 — 实时收集通信流量数据

1．各方应采取必要的法律措施和其他措施，以使具有法定资格的主管部门能够：

a. 在该签约方管辖氛围内，通过技术手段的应用来收集或记录；以及

b. 迫使服务提供商在其现有的技术能力范围内：

i. 在该签约方管辖氛围内，通过技术手段的应用来收集或记录；或者

ii. 合作和协助主管部门，实时收集或记录在其管辖范围内通过计算机系统传递的、与特定通信有关的通信流量数据。

[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．鉴于签约方国内法律体系已确立的原则，当签约方无法采取第 1.a 段中提及的措施时，该签约方可以改为采取必要的法律措施和其他措施，以确保实时收集或记录在其管辖范围内通过技术手段传递的、与特定通信有关的通信流量数据。

3．各方应采取必要的法律措施和其他措施，责成服务提供商为本条款中规定的任何权力的执行事实以及与之相关的任何信息保守秘密。

4．在本条款中提及的权力与程序应服从第 14 条和第 15 条。

第 20 条包含用于收集通信流量数据的两种不同方法，两者都假定得到执行。[1465]

- 第一种方法是履行国际互联网服务提供商的一项义务，使执法机构能够直接收集相关数据。这通常要求安装一个接口，使执法机构能够用来访问国际互联网服务提供商的基础设施。[1466]
- 第二种方法是使执法机构能够迫使国际互联网服务提供商收集执法机构要求的数据。这种方法使调查人员能够利用提供商一般已具备的现有技术能力和知识。将这两种方法相结合，其意图之一是确保在提供商不具备记录数据的相关技术时，执法机构应能在没有提供商的协助下完成调查（基于第 20 条第 1b 小段）。[1467]

《网络犯罪公约》的起草，既不是偏爱于哪一种特殊技术，也不是打算根据相关行业高额的财政投资需要而设定一些标准。[1468] 从第 20 条第 1a 小段的角度来看，《网络犯罪公约》看起来是一种更好的解决方案。不过，第 20 条 2 小段中的规定表明，《公约》的起草者认识到，有些国家可能在执行能使执法机构直接进行调查的法律方面存在困难。

根据第 20 条，调查中的主要困难之一是，匿名通信手段的使用。如上面所解释的那样，[1469] 违法者可使用国际互联网中的服务，这些服务使匿名通信成为可能。如果违法者使用诸如 TOR 软件 [1470] 之类的匿名通信服务，那么在大多数情况下，调查人员将无法成功地分析通信流量数据和确定通信参与者。使用公共国际互联网终端，违法者可以达到同样的效果。[1471]

相比传统的搜查和查封程序，收集通信流量数据的优势之一在于，犯罪嫌疑人不一定意识到正在进行的调查。[1472] 这限制了其操纵或删除证据的可能性。为确保服务提供商不会告知违法者有关正在进行的调查，第 20 条第 3 小节解决了这一问题，并责成各签约国执行一些法律，以确保服务提供商保证保守其了解的、有关正在进行的调查的秘密。对服务提供商而言，这带来了一个优点，即提供商从告知用户 [1473] 的义务 [1474] 中解放出来了。

[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.

[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.

《网络犯罪公约》旨在改进和协调各国与网络犯罪有关的法律方面问题。[1475] 在这一背景下，重要的是强调，根据《公约》第 21 条，该条款不仅适用于与网络犯罪有关的违法行为，还适用于任何违法行为。电子通信的使用不仅与网络犯罪案件相关，对网络犯罪违法行为之外的调查，这一条款也是有用的。例如，这将使执法机构能够使用通信流量数据，它们是在准备传统犯罪期间、在违法者之间交换电子邮件时产生的。第 14 条 3 小段使各方能够做出保留，并将条款的应用限于某些违法行为。[1476]

《英联邦计算机以及与计算机有关的犯罪的示范法》：

在 2002 年版的《英联邦示范法》中可以找到一种类似的方法。[1477]

> （1）如果警官对与一次特定通信相关的通信流量数据确信其必要性，出于犯罪调查目的而合理要求提供，那么警官可以通过书面的形式通知控制此类数据的人，要求此人：
>
> （a）收集或记录在某个特定期限内、与特定的通信相关的通信流量数据；以及
>
> （b）允许和协助某位特定的警官收集或记录该数据。
>
> （2）如果地方法官对[法院上宣过誓的][书面陈述的][信息]确信其必要性，对[嫌疑人]合理推断，认为存在通信流量数据，出于犯罪调查目的而合理要求提供，那么地方法官[可][应]授权一位警官，通过运用技术手段，来收集或记录在某个特定期限内、与特定的通信相关的通信流量数据。

6.2.10 截获内容数据

《网络犯罪公约》：

除了第 21 条涉及内容数据这一事实，其结构也类似第 20 条。如果执法机构已经知道谁是通信参与者，但不知道要交换的信息类型，那么在这些情况下，截获数据交换过程的可能性就十分重要。第 21 条使他们有可能记录数据通信并对其内容进行分析。[1478] 这包括从网站上或文件共享系统中下载的文件、由违法者接收或发送的电子邮件以及聊天记录。

[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.

[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.

第 21 条 – 截获内容数据

1．与由本国法律确定的严重违法行为的范围有关，各方应采取必要的法律措施和其他措施，以使其具有法定资格的主管部门能够：

a. 在该签约方的管辖范围内，通过技术手段的应用进行收集或记录，以及

b. 迫使服务提供商，在其现有的技术能力范围内：

i. 在该签约方的管辖范围内，通过技术手段的应用进行收集或记录；或者

ii. 合作和协助主管部门，实时收集或记录在其管辖范围内通过计算机系统传递的、特定通信的内容数据。

2．鉴于签约方国内法律体系已确立的原则，当签约方无法采取第 1.a 段中提及的措施时，该签约方可以改为采取必要的法律措施和其他措施，以确保实时收集或记录在其管辖范围内通过技术手段传递的、特定通信的内容数据。

3．各方应采取必要的法律措施和其他措施，责成服务提供商为本条款中规定的任何权力的执行事实以及与之相关的任何信息保守秘密。

4．在本条款中提及的权力与程序应服从第 14 条和第 15 条。

与通信流量数据的情况不同，《网络犯罪公约》没有提供内容数据的定义。“内容数据”这一术语指的是通信的内容。

在网络犯罪调查过程中，内容数据的例子包括：

- 电子邮件的主题；
- 嫌疑人打开过的网站内容；
- VoIP 交谈的内容。

根据第 21 条，调查的最大困难之一在于加密技术的使用。[1479] 正如之前所详细解释的那样，加密技术的使用使违法者能够以一种执法机构无法访问的方式来保护内容数据。如果受害者对其传输的内容进行了加密，那么违法者只能截获经过加密的通信，而无法分析其内容。由于无法访问加密文件中使用的密钥，可能的解密也要花非常长的时间。[1480]

[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.

[1480] *Schneier*, Applied Cryptography, Page 185.

《英联邦计算机以及与计算机有关的犯罪的示范法》：

在 2002 年版的《英联邦示范法》中可以找到一种类似的方法。[1481]

> **截获电子通信**
>
> 18.（1）如果地方法官对[法院上宣过誓的][书面陈述的][信息]确信其必要性，对[嫌疑人]合理推断，[认为]电子通信的内容是出于调查犯罪的目的而合理要求的，那么地方法官[可][应]:
>
> （a）命令[制定法律国家]提供国际互联网服务的提供商通过技术手段的运用来收集或记录、或者允许或协助主管部门来收集或记录内容数据，这些内容数据与借助计算机系统手段进行的特定通信相关；或者
>
> （b）授权一位警官，通过运用技术手段来收集或记录该数据。

6.2.11 有关加密技术的规定

如上所述，通过使用加密技术，违法者也可以阻止对内容数据的分析。各种各样的软件产品可以使用户有效地保护文件以及数据传输过程，使之免受未授权的访问。[1482] 如果嫌疑人使用这样一种产品，而调查机构无法访问到用于加密文件的密钥，那么所需的解密可能要花很长时间。[1483]

违法者使用加密技术对执法机构而言是一个挑战。[1484] 各种各样的国家方法和国际方法 [1485] 都在寻求解决这一问题。[1486] 由于对加密技术威胁的估计不同，迄今为止，对这一问题，还没有一种被广泛接受的国际方法。最常用的解决方案有：

[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.

- 在犯罪调查中，执法机构需要获得授权，在必要时破解密码。[1487] 没有此类授权，或者不具备发布提供数据命令的可能性，则调查机构可能无法收集必要的证据。此外，或者作为一种选择方案，调查人员可以获得授权来使用键盘记录器软件，以截获加密文件的通关密码，以破解加密。[1488]

- 通过限制密钥长度，这一规则限定了加密软件性能。[1489] 取决于限制的程度，这将使调查人员能在合理的时间内破解密钥。此类解决方案的反对者担心这些限制将不仅使调查人员能够破解密码，而且使那些试图刺探加密商业信息的经济间谍也具备了这种能力。[1490] 此外，如果此类软件工具不可用，那么限制只能阻止违法者使用更强大的加密技术。这将首先要求采用国际标准，以防止功能强大的加密产品的制造商在没有适当限制密钥长度的国家里提供他们的产品。不管怎样，违法者都可能相对容易地开发出他们自己的、不限制密钥长度的加密软件。

- 要为强大的加密产品建立密钥第三方系统或密钥恢复程序。[1491] 此类制度的实施将使用户能够继续使用强大的加密技术，但也使调查人员能够访问到相关的数据，方法是迫使用户向保存密钥的专门机构提供它们，并在必要时将其提供给调查人员。[1492] 这样一种解决方案的反对者担心，违法者可能访问到所提交的密钥，并用它们来解密秘密信息。此外，通过开发其自身的加密软件，无需向主管部门提供密钥，违法者可比较容易地绕过这一规定。

- 另一种方法是提供数据命令。[1493] 这一术语描述透露用于加密数据的密钥的义务。1997 年在美国丹佛召开的八国集团峰会期间对此类手段的实施情况进行了讨论。[1494] 许多国家已经开始实施此类义务。[1495] 国家层面执行情况的一个例子是 2000 年版的《印度信息技术法案》第 69 节。[1496] 此类义务的一个例子是 2000 年版的《英国调查权规定》第 49 节：[1497]

[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: 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,

第 49 节

（1）本节适用于任何受保护的信息。

（a）该信息已被某人拥有，此人借助履行法定权力的手段来查封、扣留、检查、搜查或以其他方式干扰文件或其他财产，或者可能这样做；

（b）该信息已被某人拥有，此人借助履行某种法定权力的手段来截获通信，或者可能这样做；

（c）该信息被某人拥有，此人借助履行依据第 22（3）节或依据第 II 部分中的授权而赋予的某种权力的手段，或者是依据第 22（4）节发出通知的结果，或者可能这样做；

（d）该信息被某人拥有，是依据某种法定职责（不管是否因请求信息而产生）而提供或透露的结果，或者可能这样做；或者

（e）借助任何其他不涉及法定权力履行的法律手段，该信息已被某个情报机构、警察或者海关官员和税务官员拥有；或者可能被任何此类机构、警察或者海关官员和税务官员拥有。

（2）如果根据日程表 2，拥有适当许可的任何人，根据合理的理由认为 —

（a）受保护信息的密钥可以归任何人所有，

（b）迫使其接受透露受保护信息的要求：

（i）根据第（3）小节的理由认为是必要的，或者，

（ii）某个公共主管部门，出于保证有效履行或适当行使某种法定权力或法定职责的目的，认为是必要的，

（c）迫使其接受这样一个要求与这种强迫要求旨在达到的目标之间是均衡的，以及

（d）对于获得适当许可、以可理解的形式获得受保护信息的人，如果未依据本节发出通知，那么不是合理可行的，拥有这种许可的人可以通过通知他认为拥有密钥的人，强迫要求他透露受保护的信息。

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.

（3）针对任何受保护信息的透露要求，根据本小节中的理由认为是必要的，如有必要 —

（a）出于国家安全的考虑；

（b）出于预防或侦查犯罪的目的；或者

（c）出于英国的经济利益。

（4）依据本节强迫要求透露任何受保护信息的要求的通知 —

（a）必须以书面方式进行提供，或者（如果不是以书面形式）必须以能够对其已经提供这一事实形成记录的方式进行提供；

（b）必须描述通知涉及的受保护信息；

（c）通过参考所提供的通知，必须详细说明第（2）（b）（i）或（ii）小节中所述的各个事项；

（d）必须详细说明通知发出人所持有的职务、官阶或职位；

（e）必须详细说明出于日程表 2 之目的授权发出通知的人的职务、官阶或职位；或者（如果发出通知的人有权在未获得他人许可的情况下发出通知）必须描述引发其授权的情形；

（f）必须详细说明通知需遵守的时间；以及

（g）必须陈述通知要求的透露，以及透露的形式和方式；以及出于第（f）段的目的而规定的时间必须允许在所有情况下都能合理地遵照执行。

为确保负责透露密钥的人遵照命令并真正提交密钥，2000 年版的《英国调查权法案》包含一条有关对未遵守命令的人进行定罪的条款。

第 53 节

（1）收到第 49 节通知的人，如果有意不遵守该通知，没有根据通知透露通知中要求的信息，那么认为他违法。

（2）在根据此节对任何人的违法行为进行起诉的过程中，如果有证据表明，此人在第 49 节的通知发出之前的任何时间内，拥有针对任何受保护信息的密钥，出于那些起诉的目的，此人应被视为在此后的所有时间内都继续拥有该密钥，除非有证据表明在发出通知之后以及他被要求透露密钥之前，他并不拥有密钥。

（3）出于本节的目的，如果是以下几种情形，那么当事人将被视为已经表明他不拥有针对受保护消息的密钥 —

（a）该事实的足够证据被举出，导致了涉及它的一个问题；以及

（b）相反的情形未被证明超出了合理的疑问。

（4）在根据此节对任何人的违法行为进行起诉的过程中，如果当事人能够表明以下事项，那么应作为一种辩护：

（a）对他而言，要按照第 49 节中提供的通知要求，在规定的时间之前按照该通知要求透露数据并非合理可行；但是

（b）在那一时间之后，他立即进行了透露，原因是对他而言，这样做才是合理可行的。

（5）根据本节，对违法之人应处以 —

（a）在被判有罪被提起控告的情况下，判处不超过两年的监禁或者一定数额的罚款，或者两项并罚；

（b）根据简易判决定罪，判处不超过六个月的监禁或者不超过法定最大数额的罚款，或者两项并罚。

2006 年版的《调查权法案规定》责成犯罪嫌疑人支持执法机构的工作。对该规定，主要有三个方面的考虑：

- 一个通常的担心涉及以下事实，即该义务可能导致与自我认罪的嫌疑人的基本权利产生冲突。[1498] 不是将调查留给主管部门，而是嫌疑人需要为调查提供主动支持。在许多国家，对自我认罪有很强的保护，这产生了问题，即此类规定究竟有多大的潜力可成为一种示范解决方案，用于解决与加密技术有关的挑战。
- 另一个担心涉及以下事实，即丢失该密钥可能导致犯罪调查。尽管定罪要求违法者有意拒绝透露密钥，但丢失密钥可能导致使用加密密钥的人招来不希望的刑事起诉。但特别是第 53 节第 2 小段，潜在地干扰了提供证据的责任。[1499]
- 有一些技术解决方案能使违法者躲避透露用于加密数据的密钥的义务。违法者可以躲避这种义务的一个例子是，根据“似是而非的否认能力”原则使用加密软件。[1500]

[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.

[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.

6.2.12 远程取证软件

如上所解释的那样，在嫌疑人的计算机上搜查证据，要求物理访问相关的硬件（计算机系统和外部存储介质）。这一程序通常伴随要求进入嫌疑人的公寓、住所或办公室。在这种情况下，当调查人员开始进行搜查时，嫌疑人将在同一时刻意识到正在进行的调查。[1501] 这一信息可能导致行为的改变。[1502] 比如，如果嫌疑人攻击某些计算机系统，以检验他的能力，以便与其他违法者一道参与对未来某一时候更大规模攻击的准备，那么搜查程序可能阻碍调查人员确定其他嫌疑人，原因是这位违法者很有可能将停止与他们的通信。

为了避免嫌疑人察觉正在进行的调查，执法机构需要一种手段，使他们能够访问存储在嫌疑人计算机中的计算机数据，而且该手段可以秘密使用，好比用于监控电话呼叫的电话监听技术。[1503] 这样一种手段将使执法机构能够远程访问嫌疑人的计算机并搜查信息。当前，正在激烈讨论此类工具是否必要这一问题。[1504] 2001 年，已有报告指出，美国联邦调查局（FBI）正在开发一种称为“摩幻灯笼”的键盘记录器工具，以便用于与国际互联网有关的调查。[1505] 2007 年发表的一些报告指出，美国的执法机构正使用软件来跟踪运用匿名通信手段的嫌疑人。[1506] 这些报告指的是在使用一种称为 CIPAV [1507] 的工具时要求提供搜查证。[1508] 在德国联邦法院决定现有的《刑事程序法》条款不允许调

[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 (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

查人员使用远程取证软件来秘密搜查嫌疑人的计算机后，关于在这一领域是否需要修改现有法律条款的争论就开始了。[1509] 在这一争论中，公开了调查机构曾非法使用远程取证软件来进行一些调查的消息。[1510]

对“远程取证软件”的各种各样概念、尤其是它可能具备的功能，一直在讨论中。[1511] 从理论的角度来看，这种软件可能具备以下功能：

- 搜查功能 — 该功能将使执法机构能够搜查非法内容并收集有关计算机上所存文件的信息。[1512]
- 记录 — 调查人员可以记录曾在嫌疑人的计算机系统中处理过的数据，而无需这些数据永久地保存。比如，假使嫌疑人使用网络语音服务（VoIP）来与其他嫌疑人通话，那么其交谈内容一般不会保存。[1513] 远程取证软件可以记录这种经过处理的数据，为调查人员保存它们。
- 键盘记录器 — 如果远程取证软件包含一个模块来记录键击，那么该模块可以用于记录嫌疑人用来加密文件的密码。[1514]
- 身份识别 — 这一功能使调查人员能够证明嫌疑人参与了某一犯罪行为，即使他使用匿名通信服务来阻止调查人员通过跟踪所用的 IP 地址来确定违法者。[1515]
- 激活外设 — 远程取证软件可用来激活用于室内监视目的的摄像头或麦克风。[1516]

尽管这种软件可能的功能看起来对调查人员十分有用，重要的是指出，这类软件的使用存在许多法律上和技术上的困难。从技术角度来看，需要考虑到以下几个方面的问题：

- 涉及安装过程的困难 — 这种软件需要安装在嫌疑人的计算机系统上。恶意软件的广泛传播证明，不经过国际互联网用户的许可而在其计算机上安装软件是可以做到的。但病毒与远程取证软件的主要区别在于，远程取证软件需要安装在某个特定的计算机系统（嫌疑人的计算机）上，而计算机病毒旨在感染尽可能多的计算机，无需聚焦于某一个特定的计算机系统。至于如何将软件传输到嫌疑人的计算机上，存在许多方法。例如：物理访问计算机系统而安装；将软件放在网站上供下载；通过绕过安全措施在线访问计算机系统；以及在国际互联网活动期间产生的数据流中隐藏该软件，还有其他一些方法，提到的只是一小部分。[1517] 由于大多数计算机

---

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.

[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.

配备了如病毒扫描软件和防火墙之类的保护措施，因此对调查人员而言，所有的远程安装方法都将面临困难。[1518]

- 物理访问的优点 — 已开展的大量分析（如物理检查数据处理介质）要求访问硬件。此外，远程取证软件只能使调查人员分析连接到国际互联网的计算机系统。[1519] 此外，难以保持嫌疑人计算机系统的完整性。[1520] 至于这些方面问题，远程取证软件通常不能代替对嫌疑人计算机系统进行物理检查。

此外，在执行一项规定使调查人员能够安装远程取证软件之前，还需要考虑大量的法律问题。在许多国家，《刑事程序法》以及《宪法》中确定的保护措施，限制了此类软件的潜在功能。除了国家层面的问题之外，远程取证软件的安装可能侵犯国家主权原则。[1521] 如果软件安装在一部笔记本电脑中，而在安装过程后该电脑被带到了国外，那么该软件可能使调查人员能够在没有获得有关当局必要许可的情况下，在外国管辖范围内进行犯罪调查。

6.2.13 授权要求

违法者可以采取一些措施，使调查变得复杂。除了使用一些能够进行匿名通信的软件外，[1522] 如果嫌疑人使用公共国际互联网终端或者开放无线网络，那么对其身份的识别可变得很复杂。对一些能使用户隐藏其身份的软件生产的限制，以及对无需身份验证的公共国际互联网接入终端的限制，可以使执法机构更有效地开展调查。限制使用公共终端来实施犯罪的一种方法的例子是《意大利法令 144》[1523] 的第 7 条，[1524] 它已于 2005 年转变成一部法律（法律代号 155/2005）。[1525] 这一条款强迫打算提供公共国际互联网接入服务的任何人（如网吧或大学 [1526] ）申请授权。此外，要求提到的人员请求其客户在接入和使用服务之前提供身份信息。至于设立无线接入点的私人通常不受该义务约束的事实，如果违法者利用未保护的私人网络来隐藏其身份，那么可非常轻易地绕过监控。[1527]

调查的改进程度是否就可证明对国际互联网接入的限制以及对匿名通信服务的限制是合理的，值得怀疑。如今，免费接入国际互联网已被认为是自由获取信息权的一个重要方面，受到多个国家

[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 electrnic 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 seqDecree 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.
[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.

《宪法》的保护。身份验证的要求可能会影响到对国际互联网的使用，原因是这样做将会使用户总担心其对国际互联网的使用受到监控。即使用户知道他们的活动是合法的，仍然有可能影响到他们的交流与使用。[1528] 与此同时，希望防止身份验证的违法者，可以轻易地绕过身份验证程序。比如，他们可以使用在国外购买的预付费电话卡，利用这种电话卡，不需要身份验证就可接入国际互联网。

6.3 国际合作

6.3.1 引言

日益增长的网络犯罪其影响波及国际范围。[1529] 如上所述，导致该现象的一个原因是出于以下事实，即攻击者几乎不需要亲临提供服务的现场。[1530] 结果是，罪犯通常无需出现在受害者所在的位置。一般地，网络犯罪调查需要国际合作。[1531] 在跨国调查中，调查者其中一个关键要求是攻击者所在国的搭档需立即做出反应。[1532] 尤其是当遇到此类问题时，传统的相互援助手段在大多数情况下无法满足国际互联网中对调查速度的要求。[1533] 《网络犯罪公约》在第 23 条至第 35 条中对越来越重要的国际合作问题进行了阐述。在《斯坦福公约》草案中可找到另一种方法。[1534]

6.3.2 国际合作的一般原则

《网络犯罪公约》第 23 条定义了在成员国间就网络犯罪调查开展国际合作的三条一般原则。

> **第 23 条 — 与国际合作有关的一般原则**
>
> 依据本章规定，各方应相互合作，通过运用与犯罪问题国际合作有关的国际机制，基于一致的或互惠的法律以及国内法律，在可能的最大程度上，为调查或起诉与计算机系统和数据有关的犯罪行为或者收集犯罪行为的电子证据，达成协定。

[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.

首先，假定各成员国将在最大可能的程度上为国际调查提供合作。该义务反映了在网络犯罪调查中国际合作的重要性。此外，第 23 条指出，一般原则不仅适用于网络犯罪调查，而且适用于任何需要收集电子证据的调查。这既涉及网络犯罪调查，也涉及传统案件的调查。如果谋杀案件中的嫌疑犯使用了国外的电子邮件服务，那么第 23 条将适用于对托管服务提供商储存之数据所做的调查。[1535] 第 3 条原则指出，与国际合作有关的规定不替代与相互法律援助和引渡有关的国际协议规定或者与国际合作有关的国内法律相关规定。《公约》的起草者强调，原则上应通过运用与相互援助有关的相关条约和类似协定，来达成相互援助。因此，只有在那些现有条约、法律和协定未包含此类规定的案件中，要求各方建立一个法律基础，以便实现如《公约》所定义的国际合作。[1536]

6.3.3 引渡

国民引渡仍是最困难的国际合作问题之一。[1537] 引渡请求常常会在需要为公民提供保护与需要为国外正在进行的调查提供支持之间造成冲突。第 24 条定义了引渡原则。不像第 23 条，规定仅限于《公约》中提到的犯罪行为，不适用于未成年人的案件（剥夺最长期限为至少 1 年的自由[1538]）。为了避免有关各方保留权利方面的冲突，第 23 条基于双重犯罪行为的原则。[1539]

第 24 条 — 引渡

1a. 本条款适用于依据本《公约》第 2 条至第 11 条所犯之犯罪行为的各方间引渡，条件是依据双方法律，这些犯罪行为是可依法处罚的，可以剥夺最长期限为至少 1 年的自由，或者更加严厉的惩罚。

b. 如果依据基于一致的或互惠的法律或者引渡条约而达成的协定，包括《欧洲引渡公约》（ETS No. 24），要采用的不同的最大惩罚在双方或多方之间适用，那么应采用依据此类协定或条约的最低惩罚。

2. 应将本条款第 1 段中所述的犯罪行为归入当前双方或多方间存在的任何引渡条约认可的、可引渡的犯罪行为。各方同意在其间达成的任何引渡条约中纳入此类犯罪行为，作为可引渡的犯罪行为。

3. 如果依据现有条约实施引渡的一方收到来自另一方的引渡请求，而该方没有这样一个引渡条约，那么可以将该《条约》作为与本条款第 1 段中所述之任何犯罪行为有关的引渡的法律基础。

[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.

4．不依据现有条约实施引渡的各方应承认本条款第 1 段中所述之犯罪行为是可以在其间引渡的犯罪行为。

5．引渡应满足被请求方法律或适用的引渡条约所规定的条件，包括被请求方可能拒绝引渡的依据。

6．如果仅仅因为被请求引渡者的国籍问题，或者因为被请求方认为它对犯罪行为拥有司法权，而拒绝与本条款第 1 段中所述之犯罪行为有关的引渡，那么出于诉讼目的，应请求方请求，被请求方应将案件提交给有法定资格的权威部门，并适时将最终结果告知请求方。这些权威部门将依据该方法律，以针对具有可比特性的任何其他犯罪行为的相同方式，来做出决定，并开展调查和诉讼。

7a．在签署或提交认可、接受、批准或同意文件时，各方应将在无条约情况下负责提出或接受引渡或临时逮捕请求的各权威部门的名称和地址，告知欧洲理事会秘书长。

7b．欧洲理事会秘书长将建立并保持最新的各方指定之权威部门的注册记录。各方确保任何时候注册记录中所存的详细信息都是正确的。

6.3.4 相互援助的一般原则

关于相互援助，第 25 条对在第 23 条中所述的原则做了补充。第 25 条中最重要的规定之一是第 3 段，它强调了在网络犯罪调查中快速通信的重要性。[1540] 如之前所指出的那样，由于调查拖得太长，并因此导致在采取程序措施保存它们之前重要数据被删去，造成许多国家层面上的网络调查失败。[1541] 需要相互法律援助的调查通常需要更长时间，原因是执法机构通信中的形式要求很费时。《公约》通过强调促成使用快速通信方式的重要性来解决该问题。[1542]

第 25 条 — 与相互援助有关的一般原则

1．为了调查或起诉与计算机系统和数据有关的犯罪行为或者收集犯罪行为的电子证据，各方应在最大可能的程度上相互提供援助。

2．各方也应采取必要的此类法律措施及其他措施，来履行第 27 条至第 35 条所述的义务。

3．在紧急情况下，各方也可以借助快速通信手段，包括传真或电子邮件，请求相互援助或进行有关通信，程度为此类手段可提供适当水平的安全保密和认证（包括必要时使用加密技术）。当被请求方提出要求时，之后应提供正式的确认。被请求方应接受和回应通过此类快速通信手段所提的请求。

[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.
[1542] See Explanatory Report to the Convention on Cybercrime, No. 256.

4．除非在本章的条款中另有特殊规定，否则相互援助应满足被请求方的法律或所用相互援助条约规定的条件，包括被请求方可能拒绝合作的依据。被请求方不得仅仅因为它认为请求所涉及的犯罪行为是一种财政方面的犯罪行为，而行使权力拒绝与第 2 条至第 11 条中所提及的犯罪行为有关的相互援助。

5．当依据本章规定，允许被请求方根据存在双重罪行这一条件来实施相互援助时，如果依据其法律正在寻求援助的犯罪行为是刑事犯罪行为，那么应认为条件是满足的，而不管其法律是将该犯罪行为归入相同的类别，还是以请求方相同的术语来命名该犯罪行为。

在国家层面上进行的网络犯罪调查中，可寻找与另一个国家有关的犯罪线索。例如，如果执法机构调查一个儿童色情案件，那么它们可以从其他国家寻找有关参与了儿童色情交易的娈童者的信息。[1543] 第 26 条描述了有关规定，以便执法机构通告外国的执法机构，而不损害其自身的调查工作。[1544]

第 26 条 — 自发信息

1．在其国内法律限制范围内，且无需事先请求，当它认为透露信息有助于接收方起动或完成与依据本《条约》所犯之刑事犯罪行为有关的调查或诉讼时，或者当它认为可依据本章的规定提出合作请求时，某一方可访问在其自身调查框架内获得的另一方信息。

2．在提供此类信息之前，提供方可请求保守信息的秘密，或者仅依据规定的条件来使用这些信息。如果接收方不能遵守此类请求，那么它应告知提供方，提供方将决定是否仍提供信息。如果接收方依据规定的条件接受信息，那么它应遵守这些条件。

第 26 条最重要的规定之一与信息机密性有关。考虑到以下事实，即许多调查只能在攻击者未意识到调查正在进行的情况下完成，因此第 26 条使得提供方能够请求保守所传送信息的秘密。如果不能保证机密性，那么提供方可拒绝提供信息。

6.3.5 在无适用的国际协议情况下关于相互援助请求的程序

如同第 25 条，第 27 条基于以下考虑，即相互法律援助应通过相关条约和类似协定的应用来实施，而不仅仅依据《公约》。《公约》的起草者决定不在《公约》内单独建立一个强制的相互法律援助体系。[1545] 如果已有其他法律手段，那么第 27 条和第 28 条在某个具体的请求内并不相关。只有在其他规定不适用的案件中，第 27 条和第 28 条才提供了一套可用于实施相互法律援助请求的机制。

[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.
[1545] See Explanatory Report to the Convention on Cybercrime, No. 262.

第 27 条管制的最重要的问题包括：

- 为相互法律援助请求建立一个指定联络点的义务；[1546]
- 联络点之间直接通信的要求，以避免程序冗长；以及 [1547]
- 欧洲理事会秘书长负责创建一个包含所有联络点的数据库。

此外，第 27 条还定义了有关援助请求的限制条件。特别地，当遇到以下情况时，《公约》各方可拒绝合作：

- 政治性的犯罪行为；和/或
- 如果认为合作可能有损主权、安全、公共秩序或其他基本权益。

《公约》起草者一方面认为应使各方能在某些案件中拒绝合作，但另一方面又指出，各方应有限制地行使拒绝合作权力，以避免与之前所述的原则产生冲突。[1548] 因此，尤其重要的是，需精确定义“其他基本权益”这一术语。《网络犯罪公约的说明性报告》指出，可以是以下案件，即合作将给被请求方带来根本性的困难。[1549] 从起草者的角度来看，不认为与不适当的数据保护法律有关的利害关系是基本权益。[1550]

6.3.6 关于临时措施的相互援助

第 28 条至第 33 条反映了《网络犯罪公约》的程序手段。[1551] 《网络犯罪公约》包含众多程序手段，旨在改善在成员国中的调查工作。[1552] 关于国家主权的原则，[1553] 这些法律手段只能用于国家层面的调查活动。[1554] 如果调查者认为需要在其领土之外收集证据，那么它们需要请求相互法律援助。除了第 18 条之外，由第 16 条至第 21 条建立的各种法律手段在第 28 条至第 33 条中都有一对应的规定，使执法机构在请求外国的执法机构时能运用这些程序手段。

[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] [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.
[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).

程序手段	对应的 ML 规定
第 16 条—加速保存所储存的计算机数据 [1555]	第 29 条
第 17 条—加速保存与部分透露通信流量数据 [1556]	第 30 条
第 18 条—产品定单 [1557]	
第 19 条—搜索与捕捉所储存的计算机数据 [1558]	第 31 条
第 20 条—实时收集通信流量数据 [1559]	第 33 条
第 21 条—截获内容数据 [1560]	第 34 条

6.3.7 跨界访问所储存的计算机数据

除了纯粹反映程序规定之外，《公约》起草者还讨论了在哪些情况下允许执法机构访问那些既不储存在其领土中也不在其领土中某人控制下的计算机数据。《公约》起草者只能就两种案件情形达成协议，在这两种情形下，应由一个执法机构来完成调查工作，而无需请求相互法律援助。[1561] 不可能达成更进一步的协议，[1562] 甚至已达成的解决方案仍受到欧洲理事会成员国的批评。[1563]

允许执法机构访问储存于其领土之外的数据的这两种案件与以下相关：

- 公用的信息；和/或
- 经控制人员同意的访问。

第 32 条 — 跨国界访问允许的或公用的储存的计算机数据

无需另一方授权，一方可以：

a. 访问公用的（开放源）储存的计算机数据，而不论该数据在地理上置于何处；或者

b. 通过其领土中的一个计算机系统访问或接收位于另一方的储存的计算机数据，条件是：该方从拥有通过计算机系统透露数据给该方之法律权限的人处获得了法律上的和自愿的同意。

也不排除第 32 条未涵盖的其他情形。[1564]

[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.
[1564] See Explanatory Report to the Convention on Cybercrime, No. 293.

第 32 条指出，如果相关的数据是公用的，那么允许外国的执法机构访问该数据。公用数据的一个例子是没有访问控制（如密码）、网站上即可获得的信息。如果不允许调查者 — 不像任何其他用户 — 访问这些网站，那么将严重影响其工作。因此，应广泛接受第 32 条所述的第一种情形。

允许执法机构访问其领土之外储存的计算机数据的第二种情形是：调查者已从拥有透露数据之法律权限的人处获得了法律上的和自愿的同意。该权限受到了严厉批评。[1565] 对此规定存在激烈的争论。最重要的一点是存在以下事实，即通过建立第二种豁免情况，《公约》起草者违背了相互法律援助体系的教义结构。利用第 18 条，《公约》起草者使得调查者能够命令提交数据。由于放弃《公约》第 3 章中的相应规定，因此在国际调查中不能采用该手段。取代因允许外国的调查者直接联系数据控制者并要求提交该数据而放弃教义结构，起草者可简单地执行《公约》第 3 章中的相应规定。[1566]

6.3.8 24/7 联系网络

网络犯罪调查常常要求立即做出反应。[1567] 如上所述，当遇到确定某嫌疑犯所需的通信流量数据时，情况更是如此，原因是它们常常会在一个相当短的时间内就被删去。[1568] 为了提高国际调查的速度，《欧洲网络犯罪公约》在第 25 条中强调了使用快速通信手段的重要性。为了进一步提高相互援助请求的效率，[1569] 《公约》起草者责成各方为相互援助请求指定一个联络点，该联络点的可用性应不受时间限制。《公约》起草者强调，建立联络点是《网络犯罪公约》规定的最重要的机制之一。[1570]

第 35 条 — 24/7 网络

1．各方应指定一个 7 天、24 小时可用的联络点，以确保为与计算机系统和数据有关的刑事犯罪调查或诉讼或者收集刑事犯罪的电子证据提供即时援助。此类援助包括推动以下措施，或者其国内法律和惯例允许的话，直接实施以下措施：

a. 提供技术建议；

b. 依据第 29 条和第 30 条保留数据；

c. 收集证据、提供法律信息以及定位嫌疑犯。

[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.
[1570] See Explanatory Report to the Convention on Cybercrime, No. 298.

2a．一方的联络点应有能力完成与另一方联络点的快速通信。

2b．如果一方指定的联络点不是该方负责国际相互援助或引渡事务的权威部门的一部分，那么该联络点应确保能够快速实现与此类权威部门的协调。

3．各方应确保拥有训练有素的人员，以便推动网络运营。

24/7 网络的设想基于八国集团（G8）现有的、针对国际高技术犯罪的 24 小时联系网络。[1571] 通过创建 24/7 联络点网络，《公约》起草者旨在应对与网络犯罪作斗争所要面临的挑战 — 尤其是那些与数据交换处理[1572] 速度有关的、并具有国际影响的挑战。[1573] 要求《公约》各方建立此类联络点，并确保能够完成某些紧急行动，以及为服务提供维护。如《网络犯罪公约》第 34 条第 3 小段所述，这包括训练有素的人员。

关于联络点的建立过程、尤其是该结构的基本原则，《公约》为各成员国提供了最大的灵活性。《公约》既不要求建立一个新的权威部门，也不规定联络点可以或应该与哪个现有的权威部门相联。《公约》起草者进一步指出，24/7 网络点旨在提供技术与法律援助的事实将导致有关其实现的、各种可能的解决方案。

关于网络犯罪调查，联络点的设置有两种主要功能。这包括：

- 通过提供单个联络点，以加速通信；以及
- 通过授权联络点立即完成某些调查，已急速通信。

两种功能的结合将有望使国际调查的速度达到国家调查的速度水平。

《网络犯罪公约》第 32 条定义了网络点的最低性能要求。除了技术援助和提供法律信息之外，联络点的主要任务包括：

- 保留数据；
- 收集证据；以及
- 定位嫌疑犯。

在此也需强调，《公约》未定义应由哪个权威部门来负责 24/7 联络点的运转。如果负责联络点运转的权威部门有权命令保留数据，[1574] 以及命令某个外国的联络点请求此类保留，那么本地联络点可立即命令采取措施。如果负责联络点运转的权威部门自身无权命令保留数据，那么重要的是联络点能够直接与有权的权威部门联系，以确保立即采取措施。[1575]

在《网络犯罪公约》委员会第二次会议上明确指出，参与 24/7 联络网络不需要签署或批准《公约》。[1576]

[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.
[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).

6.3.9 《斯坦福公约》草案中的国际合作

《斯坦福公约》[1577] 草案起草者知晓网络犯罪国际影响的重要性及其面临的挑战。为了应对这些挑战，他们加入了涉及国际合作的特别规定。规定涵盖以下主题：

- 第 6 条 – 相互法律援助；
- 第 7 条 – 引渡；
- 第 8 条 – 起诉；
- 第 9 条 – 临时补救措施；
- 第 10 条 – 被控告者的权利；
- 第 11 条 – 执法过程中的合作。

该方法显示了许多与《网络犯罪公约》中所采取之方法的相同性。主要的差别在以下事实，即相比《斯坦福公约》草案，《网络犯罪公约》的规定更加严格、更加复杂、定义得更加准确。如《斯坦福公约》草案起草者所提出的那样，《网络犯罪公约》的方法更加实用，因此，在实际应用中具有某些明显的优势。[1578] 《斯坦福公约》草案起草者决定采用一种不同的方法，原因是他们预测，新技术的实施将带来某些困难。结果是，它们只提出一些一般性的指令，而不对其做更细的规定。[1579]

6.4 国际互联网提供商的责任

6.4.1 引言

即使攻击者单独行动，网络犯罪也很自然地会涉及众多人员和业务。由于国际互联网的结构，传送一个简单的电子邮件也需要众多提供商的服务。[1580] 除了电子邮件提供商之外，传送还涉及接入提供商以及负责将电子邮件转送给接收者的路由器。关于下载包含儿童色情内容的电影，情形类似。下载过程涉及上载图片（如在某个网站上）的内容提供商、为网站提供存储介质的托管服务提供商、将文件转送给用户的路由器，以及最终使用户能够访问国际互联网的访问提供商。

[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.

[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.

由于这涉及多方，因此国际互联网服务提供商一直以来关注涉及使用 ISP 服务来实施犯罪的攻击者的刑事调查。[1581] 这样做的主要理由之一是基于以下事实，即即使攻击者在国外实施犯罪，位于国境内的提供商也是犯罪调查的一个适当主体，而不冒犯国家主权原则。[1582]

一方面是网络犯罪若无提供商的介入将无法实施的事实，另一方面是提供商往往无法阻止网络犯罪的事实，使得出现这样的问题，即对国际互联网提供商的责任是否需做限制。[1583] 问题的答案对信息通信技术基础设施的经济发展至关重要。如果能够避免被用于网络犯罪，那么提供商就能在其正常的工作模式下经营业务。此外，执法机构对此问题也有极大的兴趣。执法机构的工作常常依赖于国际互联网提供商的合作。限制国际互联网提供商的责任引发了若干问题，原因是其用户的行为将影响 ISP 对网络犯罪调查的合作和支持，以及可切实防止犯罪。

6.4.2 美国方法

一方面可采取不同的方法来平衡需要提供商主动介入调查的需求，另一方面需要限制第三方行为的刑事责任风险。[1584] 可以在 17 U.S.C. §517（a）和（b）中找到一个有关法律方法的例子。

> **§512. 与在线材料有关的限制**
>
> **（a）短暂的数字网络通信**
>
> 如果：
>
> （1）由服务提供商之外的人来起动材料传输，或者在服务提供商之外的人的方向上来传输材料；
>
> （2）传输、路由、提供连接或储存通过一个自动的技术过程来完成，无需服务提供商选择材料；
>
> （3）除非自动响应另一人的请求，否则服务提供商无需选择材料的接收者；
>
> （4）不得以以下方式在系统或网络中保留服务提供商在此类中间的或短暂的储存过程中生成的任何材料拷贝，即预期接收者之外的其他人员可以以通常方式来访问这些拷贝，也不得以以下方式在系统或网络中保留任何此类拷贝，既预期接收者可以以通常方式、以比传输、路由或提供连接所需的合理时间更长的时间来访问这些拷贝；以及
>
> （5）不对通过系统或网络传输的材料内容做任何修改。
>
> 那么：
>
> 服务提供商无需承担货币援助的责任，或者除非如（j）小节所述，因提供商通过服务提供商控制或运营的系统或网络传输材料、路由材料或为材料提供连接，或者因在此类传输、路由或提供连接过程中中间地和短暂地储存该材料，而造成对版权的侵犯，则需承担指令性的或其他公平合理的援助责任。

[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."

（b）系统缓冲

如果：

（A）服务提供商之外的人可在线获得材料；

（B）（A）小节中所述之人通过系统或网络将材料传输给（A）小节中所述之人之外的人，传输方向在后者方向上；以及

（C）储存通过一个自动的技术过程来完成，目的是使材料可用于系统或网络用户，在如（B）小节所述完成材料传输后，如果满足第（2）段中所述的条件，那么用户请求访问来自（A）小节所述之人的材料。

那么：

（1）责任限制。一 服务提供商无需承担货币援助的责任，或者除非如（j）小节所述，因在服务提供商控制或运营的系统或网络中间地和临时地储存该材料，而造成对版权的侵犯，则需承担指令性的或其他公平合理的援助责任。

该规定基于 1998 年写入法律的 DMCA（数字千年版权法案）。[1585] 通过创建一个安全港体系，DMCA 自第三方排除了提供商因某些业务的版权侵权而需承担的责任。[1586] 在此，最重要的是要强调，不是所有的提供商都涵盖在限制条件的范围内。[1587] 责任限制仅适用于服务提供商[1588] 和缓冲提供商。[1589] 此外，重要的是要指出，责任是与某些要求相联的。对服务提供商的要求是：

- 由服务提供商之外的人来起动材料传输，或者在服务提供商之外的人的方向上来传输材料；
- 传输通过一个自动的技术过程来完成，无需服务提供商选择材料；
- 服务提供商无需选择材料的接收者；
- 不得以以下方式在系统或网络中保留服务提供商在此类中间的或短暂的储存过程中生成的任何材料拷贝，即预期接收者之外的其他人员可以以通常方式来访问这些拷贝。

可以在 47 U.S.C §230（c）中找到另一个有关国际互联网提供商责任限制的例子，它基于《通信礼仪法案》：[1590]

[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 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;

§230. 个人阻断和屏蔽无礼材料的保护措施

（c）“好心人”阻断和屏蔽无礼材料的保护措施

（1）发布者或发言者的处置

任何交互式计算机服务的提供商或用户都不得被看作是另一个信息内容提供商所提供之任何信息的发布者或发言者。

（2）民事责任

任何交互式计算机服务的提供商或用户都不得因以下原因而承担责任：

（A）真诚和自愿采取的任何行动，以限制访问或触及提供商或用户认为淫秽的、下流的、色情的、丑恶的、过于暴力的、扰乱的或有伤风化的材料，不论在宪法上此类材料是否受到保护；或者

（B）采取的任何行动，以使信息内容提供商或其他人可利用技术手段来限制访问段落（1）中所述的材料。

两种方法，17 U.S.C. §517（a）和 47 U.S.C §230（c），都共同关注有关特殊提供商群体和特殊法律领域的责任。因此，本章的剩余部分将概述欧盟所采用的法律方法，它遵循一个更宽的概念。

6.4.3 欧盟有关电子商务的指令

用于监管国际互联网提供商的法律方法的一个例子是欧盟的《电子商务指令》。[1591] 面对与国际互联网国际影响力有关的挑战，《指令》起草者决定制定法律标准，为信息社会的全面发展提供一个法律框架，并在此支持下实现全面的经济发展以及开展执法机构的工作。[1592] 有关责任的规定基于分级责任的原则。

《指令》包含许多用于限制某些提供商责任的规定。[1593] 限制与提供商所运营的不同类别的服务有关。[1594] 在所有其他情况下，不必排除责任，除非责任受限于其他规定，否则参与者负全责。《指令》的动机是限制在以下情况下的责任，即提供商只有有限的可能性来防止犯罪。有限可能性的原因可以是技术性的原因。例如，在速度没有大的损失的情况下，路由器无法过滤通过的数据，以及几乎不能阻止数据交换过程。如果意识到犯罪行为，那么托管服务提供商能够删去数据。不过，像路由器一样，大的托管服务提供商无法控制其服务器上储存的所有数据。

关于实际控制犯罪行为的不同能力，托管服务提供商和接入提供商的责任是不同的。关于这点，需要考虑的是以下事实，即《指令》的平衡基于现有的技术标准。当前，没有任何工具可用来自动探测未知的色情图像。如果该领域的技术继续发展，那么可能有必要在未来对提供商的技术能力作出评估，必要的话，对系统进行调整。

[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:

6.4.4 访问提供商的责任（欧盟指令）

第 12 条至第 15 条定义了对不同提供商责任的限制程度。基于第 12 条，只要满足第 12 条中定义的三个条件，就可以完全排除接入提供商和路由器运营商的责任。结果是，接入提供商一般不对其用户所犯的罪行负责。如果法院或主管部门命令，那么这种完全排除责任并不意味将免除提供商防止进一步犯罪的义务。[1595]

第 12 条 — “仅仅是传输”

1．当提供信息社会服务时，服务由在通信网络中传送服务接受者所提供的信息组成，或者提供对通信网络的接入，各成员国应确保服务提供商不对所传输的信息负责，条件是：

（a）提供商不起动传输；

（b）提供商不选择传输的接收者；以及

（c）提供商不选择或修改传输中所包含的信息。

2．第 1 段中所指的传输和提供接入行为包括自动地、中间地和短暂地储存所传输的信息，至于此行为的目的，只是为了完成在通信网络中的传输，并假定信息的保存时间不会超过传输所需的合理时间。

3．本条款不得影响法院或主管部门依据成员国法律制度要求服务提供商终止或防止侵权的可能性。

该方法可比 17 U.S.C. §517（a）。[1596] 两条规定都旨在明确说明服务提供商的责任，并且两条规定的责任限制都与类似的要求相关。主要的差别在以下事实，即第 12 条《欧盟电子商务指令》不受限于版权侵权，但排除有关任何类型犯罪的责任。

6.4.5 缓冲的责任（欧盟指令）

术语“缓冲”在此用于描述在本地存储介质上储存流行网站，以便降低带宽，使数据访问更高效。[1597] 一种用于降低带宽的技术是安装代理服务器。[1598] 在此范畴内，代理服务器可以为请求提供服务，而无需通过之前的某个请求检索保存在本地存储介质上的内容来联络特定的服务器（由用户输入域名）。《指令》起草者知晓缓冲的经济重要性，并决定：如果提供商遵守第 13 条定义的各条件，那么排除有关自动临时储存的责任。条件之一是提供商遵守有关信息更新的、被广泛认可的各标准。

[1595] See Art. 12 paragraph 3 E-Commerce Directive.
[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.

第 13 条 – “缓冲”

1．当提供信息社会服务时，服务由在通信网络中传送服务接受者所提供的信息组成，各成员国应确保服务提供商不对自动的、中间的和临时的信息储存负责，这种储存的目的仅仅是为了使应其他服务接受者的请求而进行的信息转交更高效，条件是：

（a）提供商不修改信息；

（b）提供商在访问信息时遵守各条件；

（c）提供商遵守有关信息更新的各规则，这些规则以广泛认可的和业界使用的方式来规定；

（d）提供商不干扰对业界广泛认可的和使用的技术的合法使用，以便在信息使用中获得数据；以及

（e）一旦确知以下事实，即已从网络中删去传输初始源的信息，或者已切断对之的访问，或者法院或主管部门已命令此类删去或切断，则提供商应立即行动，删去信息或者切断对之的访问。

2．本条款不得影响法院或主管部门依据成员国法律制度要求服务提供商终止或防止侵权的可能性。

《欧盟电子商务指令》第 13 条是另一个有关美国方法与欧洲方法在教义结构之间存在相似性的例子。欧盟的方法可比 17 U.S.C. §517（b）。[1599] 两条规定都旨在明确说明缓冲提供商的责任，并且两条规定的责任限制都与类似的要求相关。关于服务提供商的责任，[1600] 两种方法之间的主要差别在以下事实，即第 13 条《欧盟电子商务指令》的应用不受限于版权侵权，但排除有关任何类型犯罪的责任。

6.4.6 托管服务提供商的责任（欧盟指令）

特别地，关于非法内容，托管服务提供商在犯罪实施方面起着重要作用。将非法内容放在网上的攻击者一般不会将这些内容储存在自己的服务器上。大多数网站储存在托管服务提供商提供的服务器上。任何想经营一个网页的人都可以从托管服务提供商处租用存储容量，以保存网站。一些提供商甚至提供广告赞助的、免费的网络空间。[1601]

[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.

确定非法内容对托管服务提供商而言是一个挑战。尤其对拥有众多网站的、广受欢迎的提供商而言，在如此巨大数量的网站上手工搜索非法内容是不可能的。结果是，《指令》起草者决定限制托管服务提供商的责任。不过，不像接入提供商的情况，不免除托管服务提供商的责任。只要托管服务提供商不确切了解非法活动或其服务器上所存的非法内容，那么是没有责任的。在此假设非法内容可能储存于服务器上并不认为等同于确切了解该问题。如果提供商具体了解非法活动或非法内容，那么只有立即删去非法信息，它才能免除责任。[1602] 未能立即做出反应将导致托管服务提供商需要承担责任。[1603]

第 14 条 — 托管服务

1．当提供信息社会服务时，服务由储存服务接受者提供的信息组成，各成员国应确保服务提供商不对应服务接受者的请求而储存的信息负责，条件是：

(a) 提供商不确切了解非法活动或信息，至于要求赔偿损失，不知道非法活动或信息从何事实或何情形处显现；或者

(b) 一旦了解或指导此类情况，提供商将立即行动，删去信息或切断对信息的访问。

2．当服务接受者受制于提供商时，第 1 段将不适用。

3．本条款不得影响法院或主管部门依据成员国法律制度要求服务提供商终止或防止侵权的可能性，也不得影响成员国建立信息删去或信息访问切断监管程序的可能性。

第 14 条不仅适用于其服务限制于租用技术数据储存基础设施的提供商，也适用于流行的国际互联网服务，如提供托管服务的拍卖平台。[1604]

6.4.7 排除监控职责（欧盟指令）

在《指令》实施之前，如果可以依据与对用户行为进行监控的义务有冲突来起诉提供商，那么它在某些成员国是不确定的。除了可能与数据保护规定和电信保密规定发生冲突，此类义务将尤其会给储存有成千上万个网站的托管服务提供商带来困难。为了避免出现此类冲突，《指令》排除了有关对发送或储存信息进行监控的一般性义务。

第 15 条 — 无一般性监控义务

1．当提供第 12 条、第 13 条和第 14 条所涵盖的义务时，各成员国不得对提供商施加一般性的义务，以监控其传送或储存的信息，也不得施加要求提供商主动寻找用于指明非法活动的事实或情形的一般性义务。

2．各成员国可设立义务，要求信息社会服务提供商立即通知公共主管部门已发生的、有嫌疑的非法活动或其服务接受者提供的、有嫌疑的信息，或者设立通信义务，以便应主管部门请求，将有助于确定服务接受者的信息传送给主管部门，服务提供商与这些服务接受者之间签有储存协议。

[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.
[1604] By enabling their customers to offer products they provide the necessary storage capacity for the required information.

6.4.8 超链接的责任（奥地利 ECC）

超链接在国际互联网中起着重要作用，使得超链接提供商能够将用户导航至在线可用的特定信息上。不仅仅提供有关如何访问信息的技术细节（例如，通过提供网站域名，信息在该网站上提供），用户可以通过点击活动的超链接来直接访问信息。超链接为互联网浏览器打开沉积的国际互联网地址提供了命令。

在起草《欧盟指令》过程中，对是否需要为超链接做一规定进行了激烈讨论。[1605] 起草者决定不要求各成员国就有关超链接责任的法律达成一致。取而代之的是，实施一个再次检查程序，以确保有关超链接提供商责任之提议的需求，并考虑到定位工具服务。[1606] 在未来对超链接责任规定进行修正之前，各成员国可以自由地提出各国的解决方案。[1607] 一些欧盟国家决定在一个专门的规定中来阐述超链接提供商的责任。[1608] 这些国家基于《指令》中有关托管服务提供商责任的相同原则来处置超链接提供商的责任。[1609] 该方法是以下的逻辑结果，即认为托管服务提供商的情形与超链接提供商的情形是可比的。在两种情况下，提供商都掌控着非法内容，或者至少链接至该内容。

一个例子是奥地利 ECC 的第 17 节：[1610]

第 17 节 ECC（奥地利） — 有关超链接的责任

如果：

1．提供商不确切了解非法活动或信息，当要求赔偿损失时，不知道服务提供商从何事实或何情形处知晓活动或信息是非法的；或者；

2．一旦了解或知道此类情况，提供商将立即行动，切断电子链接。

那么：

（1）通过提供电子链接能够访问第三方提供之信息的提供商将不对信息承担责任。

[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.
[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.

6.4.9 搜索引擎的责任

通过规定某些准则，搜索引擎提供商提供搜索服务，以确定感兴趣的文件。搜索引擎将搜索与用户输入之准则相匹配的相关文件。搜索引擎在成功发展国际互联网方面发挥着重要作用。在网站上可用的、但在搜索引擎目录中未列出的内容，只有当希望访问它的人知道完整的 URL 时才能被访问到。Introna/Nissenbaum 指出，“不太夸张地说，只要存在，就会被搜索引擎查找到”。[1611]

对超链接情况，《欧盟指令》不包含定义搜索引擎运营商责任的标准。因此，一些欧盟国家决定在一个专门的规定中来阐述搜索引擎提供商的责任。[1612] 不像超链接的情况，不是所有国家的规定都基于相同的原则。[1613] 西班牙 [1614] 和葡萄牙有关搜索引擎运营商责任的规定基于《指令》第 14 条，而奥地利[1615] 则基于第 12 条来限制责任。

第 14 节 ECC（奥地利） — 有关搜索引擎运营商的责任

（1）提供搜索引擎或其他电子工具以搜索第三方提供之信息的提供商将不承担责任，条件是：

1．提供商不起动传输；

2．提供商不选择传输的接收者；以及

3．提供商不选择或修改传输中所包含的信息。

[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, ob) 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.

[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.

7. 法律参考文献

《欧洲理事会关于网络犯罪的公约》[1616]

《联邦计算机以及与计算机有关的犯罪的示范法》[1617]

《斯坦福公约》草案[1618]

[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.

瑞士印刷
2009年，日内瓦