В ПОИСКАХ КИБЕРМИРА

*Хамадун И. Туре (Hamadoun I. Touré)*

*Генеральный секретарь*

*Международного союза электросвязи*

*и*

*Постоянная группа по мониторингу*

*информационной безопасности*

*Всемирной федерации ученых*

Январь 2011 года



|  |
| --- |
| Официальное уведомление  Авторы лично обладают интеллектуальными правами на свои работы. Источники третьих сторон цитируются в соответствии с правилами. Международный союз электросвязи (МСЭ) не несет ответственности за содержание внешних источников, включая внешние веб-сайты, на которые ссылаются в данной публикации.  Ни МСЭ, ни любой другой человек, выступающий от его лица, не несет ответственности за последствия использования информации, содержащейся в данной публикации.  Правовая оговорка  Главы в данной публикации отражают мнение отдельных авторов, которые не поддерживаются или не призваны отражать мнение любой организации, в которой они могут работать или быть связаны. Упоминание и отсылки на определенные страны, компании, продукты, инициативы или руководящие указания никоим образом не означают, что они поддерживаются или рекомендованы МСЭ, авторами, или любыми другие организациями, с которыми связаны авторы, по сравнению с другими, имеющими такую же природу, которые не упоминаются.  Выражение признательности  Генеральный Секретарь МСЭ и Всемирная федерация ученых хотели бы поблагодарить Джоди Вестбай (Jody Westby), Хеннинга Вегенера (Henning Wegener) и всех авторов, которые сделали возможным собрать вместе их мнения по этой важной всемирной проблеме. Генеральный Секретарь также выражает признательность проф. Антонино Дзикики (Antonino Zichichi), президенту WFS, и свою искреннюю благодарность Главе Отдела корпоративной стратегии МСЭ Александеру Нтоко (Alexander Ntoko), и в особенности ЙонгХи Киму (JeoungHee Kim), который руководил и координировал издание данной публикации; Ребеке Льюис (Rebekah Lewis), Дипти Венкатесвар (Deepti Venkateswar), Притаму Малуру (Preetam Maloor), Марко Обизо (Marco Obiso) и Элизабет Ашенбренер (Elizabeth Aschenbrener); Клод Бриан (Claude Briand) и ее команде; и многим другим в МСЭ и WFS, без чьих вкладов эта публикация была бы невозможна |

Если у вас появятся комментарии, пожалуйста, свяжитесь с Отделом корпоративной стратегии Международного союза электросвязи, по адресу [strategy@itu.int](mailto:strategy@itu.int).

Авторское право на коллективную работу © 2011, Международный союз электросвязи и Всемирная федерация ученых

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких-либо средств без предварительного письменного разрешения МСЭ.

Содержание

**Стр.**

[**Список сокращений iii**](#_Toc289172899)

[**о Международном союзе электросвязи и Глобальной программе кибербезопасности v**](#_Toc289172900)

[**о Всемирной федерации ученых и ее Постоянной группе по мониторингу информационной безопасности vi**](#_Toc289172901)

[**Предисловие** (Хамадун И. Туре, Антонино Дзикики) **xi**](#_Toc289172902)

[**1 Введение** (Джоди Р. Вестбай) **1**](#_Toc289172903)

[**2 Киберпространство и угроза кибервойны** (Хамадун И. Туре) **7**](#_Toc289172904)

[**3 Зависимость и доверие в обществе** (Жак Бус) **14**](#_Toc289172905)

[*3.1 Зависимость современных обществ от ИКТ и интернета 14*](#_Toc289172906)

[*3.2 Социально-экономические последствия киберпреступности 26*](#_Toc289172907)

[**4 Тенденции и угрозы в технологической сфере 31**](#_Toc289172908)

[*4.1 Существующие возможности, тенденции и угрозы  
 (Аксель Лехман, Владимир Бритков, Жак Бус)* 31](#_Toc289172909)

[*4.2 Правительственная цензура интернета: Киберрепрессии  
 (Хеннинг Вегенер) 43*](#_Toc289172910)

[**5 Киберконфликт и геокиберстабильность 53**](#_Toc289172911)

[*5.1 Киберконфликт (Джанкарло А. Барлетта, Вильям А.  
 Барлетта, Виталий Н. Цыгичко) 53*](#_Toc289172912)

[*5.2 Призыв к геокиберстабильности (Джоди Р. Вестбай) 66*](#_Toc289172913)

[**6 Кибермир** (Хеннинг Вегенер) **77**](#_Toc289172914)

[*Концепция кибермира* 77](#_Toc289172915)

**Стр.**

[**7 Международный ответ кибервойне** (Хамадун И. Туре) **86**](#_Toc289172916)

[*7.1 Национальная политика и подходы 86*](#_Toc289172917)

[*7.2 Недавние международные ответные действия 91*](#_Toc289172918)

[*7.3 Необходимость международных рамок 96*](#_Toc289172919)

[*7.4 Предложения в текст Международных принципов в киберпространстве 100*](#_Toc289172920)

[**8 Глобальная программа кибербезопасности МСЭ** (Хамадун и. туре) **104**](#_Toc289172921)

[**9 Декларация Эриче по принципам киберстабильности и кибермира** (Всемирная федерация ученых) **110**](#_Toc289172922)

[**10 Заключение** (Джоди Р. Вестбай) **112**](#_Toc289172924)

# Список сокращений

AIS Автоматические информационные системы

ARPA Агентство перспективного планирования научно-исследовательских работ (Министерство обороны США)

C3 Команды, контроль и коммуникации

CoE Совет Европы

COP Инициатива по защите ребенка в онлайновой среде (МСЭ)

CRS Исследовательская служба конгресса (США)

CSCW Коллективная работа с использованием компьютеров

DARPA Агентство перспективного планирования научно-исследовательских работ в области обороны (Министерство обороны США)

DNS Система доменных имен

ECOSOC Экономический и социальный совет (ООН)

ESCAPE Прикладная платформа безопасного электронного взаимодействия для экспертов (IMPACT)

EU Европейский союз

FG Smart Фокус-группа по интеллектуальным энергосистемам

FTC Федеральная торговая комиссия (США)

GCA Глобальная программа кибербезопасности (МСЭ)

GRC Центр глобального реагирования (IMPACT)

HRC Комитет по правам человека (HRC)

ИКТ Информационные и коммуникационные технологии

IGF Форум по управлению использованием Интернета

IMPACT Международное многостороннее партнерство против киберугроз (Малайзия)

IP протокол Интернет

ISOC Интернет-сообщество

IT Информационные технологии

ITR Международное регулирование электросвязи (МСЭ)

МСЭ Международный союз электросвязи

МСЭ-T Сектор стандартизации электросвязи МСЭ

LOAC Законы вооруженного конфликта

MIT Масачуссетский технологический институт

NATO Организация Североатлантического договора

NEWS Сеть раннего предупреждения (IMPACT)

NPT Договор о нераспространении ядерного вооружения

NSF Национальный научный фонд

RFID Радиочастотная идентификация

PDA Персональный цифровой помощник

PMP Постоянная группа по мониторингу информационной безопасности (WFS)

SCADA Диспетчерский контроль и сбор данных

SOA Сервис-ориентированная архитектура

TCP Протокол управления передачей

ООН Организация Объединенных Наций

UNCPCJ Конгресс по предупреждению преступности и уголовному правосудию Организации Объединенных Наций (ООН)

UNESCO Организация Объединенных Наций по вопросам образования, науки и культуры (ООН)

UNODC Управление Организации Объединенных Наций по наркотикам и преступности (ООН)

URL Универсальный указатель ресурсов

WFS Всемирная федерация ученых

ВВУИО Всемирная встреча на высшем уровне по вопросам информационного общества

О Международном союзе электросвязи и Глобальной программе кибербезопасности

Международный союз электросвязи (МСЭ) – ведущее агентство Организации Объединенных Наций по вопросам информационных и коммуникационных технологий и глобальная точка сосредоточия внимания для правительств и частного сектора в деле разработки сетей и услуг.

Фундаментальная роль МСЭ после Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) и Полномочной конференции МСЭ 2006 года заключается в создании доверия и безопасности при использовании информационных и коммуникационных технологий (ИКТ). Главы государств и правительств, другие глобальные лидеры, участвующие в ВВУИО, а также Государства  Члены МСЭ поручили МСЭ предпринять конкретные шаги к сдерживанию угроз и опасностей, связанных с информационным обществом. Для выполнения этого поручения Генеральный секретарь МСЭ д-р Хамадун И. Туре объявил в 2007 году о начале [Глобальной программы кибербезопасности (ГПК)](http://www.itu.int/osg/csd/cybersecurity/gca/) как основы международного сотрудничества.

Цель ГПК – повысить доверие и безопасность в информационном обществе. Она разрабатывается для взаимодействия и эффективного стимулирования сотрудничества между всеми заинтересованными сторонами, и строится на существующих инициативах во избежание дублирования усилий. ГПК – это первый действительно глобально многосторонний и альянс частного и государственного секторов против киберугроз. В 2008 году МСЭ и Международное многостороннее партнерство против киберугроз (IMPACT) официально подписали Меморандум о взаимопонимании, после чего оборудованная по последнему слову техники штаб-квартира организации IMPACT в городе Сайберджая, Малайзия, стала физическим домом для ГПК. IMPACT – это международная частно-государственная инициатива, призванная расширить возможности международного сообщества по предотвращению, защите и противодействию киберугрозам. Такое взаимодействие предоставляет 192 Государствам  Членам МСЭ и другим странам опыт, оборудование и ресурсы для эффективного увеличения возможностей глобального сообщества по предотвращению, защите и противодействию киберугрозам. С самого своего начала ГПК получила поддержку и признание лидеров и экспертов в области кибербезопасности всего мира. Патронами ГПК являются Его Превосходительство д-р Оскар Ариес Санчес (Óscar Arias Sánchez), бывший Президент Республики Коста-Рика, и Его Превосходительство Блэйз Компаоре (Blaise Compaoré), Президент Буркина-Фасо.

ГПК способствует таким инициативам как Защита ребенка в онлайновой среде (COP), Ворота в кибербезопасность и, в содружестве с IMPACT и при поддержке лидирующих глобальных участников в настоящее время внедряет решения по кибербезопасности в разных странах мира. МСЭ хотел бы поблагодарить Ее Превосходительство Лауру Чинчилью, Президента Коста-Рики, за ее роль покровительницы инициативы МСЭ COP.

О Всемирной федерации ученых и ее постоянной группе по мониторингу информационной безопасности

Всемирная федерация ученых (WFS) была основана в Эриче, Сицилия в 1973 году группой известных ученых возглавляемой Исидором Исааком Раби (Isidor Isaac Rabi) и Антонино Дзикики (Антонино Zichichi). С тех пор многие ученые присоединились к Федерации, среди них Т. Д. Лии (T. D. Lee), Лаура Ферми (Laura Fermi) Евгений Виньер (Eugene Wigner) Поль Дирак (Paul Dirac) и Петр Капица (Piotr Kapitza).

Федерация WFS это свободное объединение, которое включает в себя более 10 000 ученых из **[110 стран](http://www.federationofscientists.org/WfsWorldMap.asp)**. Все ее члены разделяют одни цели и идеалы, и вносят добровольный вклад с целью поддержания принципов Федерации. Федерация способствует международному сотрудничеству в области науки и технологии среди ученых и исследователей всех частей мира – с севера, юга, востока и запада. Федерация и ее члены стремятся к идеалам свободного обмена информацией, в котором научные открытия и достижения более не ограничены малым кругом избранных. Цель состоит в обмене знаниями между людьми всех национальностей, так что каждый сможет пользоваться достижениями научного прогресса.

Создание Всемирной федерации ученых стало возможным благодаря существованию в Эриче центра научной культуры, названного в честь физика Этторе Майорана (Ettore Majorana), ***Фонда и центра научной культуры Этторе Майорана*** (Центра). Этот Центр, который получил название "Университета третьего тысячелетия", стал мировым центром образования. С момента своего создания в 1963 году Центр провел 123 школьные программы и 1497 курсов для 103 484 участников (125 из которых являются Нобелевскими лауреатами), приехавших из 932 университетов и лабораторий 140 стран.

Центр Этторе Майорана явился предшественником Всемирной федерации ученых и его действий по смягчению чрезвычайных ситуаций глобального масштаба. Всемирная федерация ученых постепенно определила 15 **чрезвычайных ситуаций глобального масштаба** и приступила к организации противодействия этим угрозам. Одним из ее главных достижений стало создание Полем Дираком, Петром Капицей и Антонино Дзикики в 1982 году Заявления Эриче, ясно определяющее идеалы Федерации и выдвигающее ряд предложений по претворению этих идеалов в жизнь. Другой важной вехой стало проведение серии Международных семинаров по проблемам ядерной войны, которые оказали огромное влияние на снижение опасности ядерной катастрофы для всей планеты и, в конечном счете, способствовали окончанию Холодной войны. В 1986 году в результате действий группы видных ученые (большая часть которых были членами WFS) была основана **Всемирная лаборатория** Международного Центра научной культуры. Всемирная лаборатория **[ICSC была](http://www.federationofscientists.org/WfsWorldLab.asp)** создана в Женеве с целью достижения целей, указанных в Заявлении Эриче.

Федерация WFS создала свою Постоянную группу по мониторингу (PMP) информационной безопасности в 2001 году. Ее отчет "*В целях всемирного порядка киберпространства: устранение угроз от киберпреступности до кибервойны*" являлся одним из руководящих документов, созданных гражданским обществом в Организации Объединенных Наций в ходе Всемирной встречи на высшем уровне по информационному обществу (ВВУИО), которая впервые была проведена в Женеве в 2003 году. Группа PMP опубликовала множество статей по кибербезопасности и кибервойнам, а также регулярно представляет проблемы информационной безопасности как важнейшую тему безопасности в масштабах планеты на пленарных заседаниях WFS, проводимых ежегодно в августе в Эриче. В августе 2009 года группа PMP была так обеспокоена возможностью того, что кибервойны разрушат общество и приведут к ненужному ущербу и страданиям, что она сформировала проект **Декларации** **Эриче о принципах киберстабильности и кибермира**, которая была одобрена Пленумом WFS по случаю 42-го собрания Международных семинаров по чрезвычайным ситуациям планетарного масштаба в Эриче 20 августа 2009 года. Декларация была разослана всем Государствам Членам Организации Объединенных Наций.

Руководителями группы PMP являются Посол Берлина и Мадрида Хеннинг Вегенер (Henning Wegener) и д-р Джоди. Р. Вестбай (Jody R. Westby) Генеральный директор ООО по глобальным киберрискам в Вашингтоне, DC. Следующие участники группы внесли свой вклад в данную публикацию:

Участники группы, внесшие вклад в данную публикацию

Вильям Барлетта (William Barletta)

Вильям А. Барлетта (William А. Barletta) исполнительный директор национальной квалификационной программы Института ускорителя элементарных частиц США. Он является адъюнкт-профессором физики в Масачуссетском технологическом институте и в Лос-Анджелесском Университете Калифорнии. Он также является приглашенным профессором экономики в университете Любляны, Словения, где он преподает стратегический менеджмент, и старший советник президента компании Sincrotrone, городе Триесте, Италия. Он является членом Американского физического общества, членом его группы по связям с общественностью, заместителем председателя его Форума по Международной физике и вице-председателем его Отдела лучевой физики. Он является соавтором и редактором пяти книг и автором более 150 статей, охватывающих очень широкий спектр технологических вопросов. [barletta@mit.edu](mailto:barletta@mit.edu)

Владимир Бритков (Vladimir Britkov)

Владимир Б. Бритков (Vladimir B. Britkov) (Ph.D.) заведующий лабораторией моделирования информации в Институте системного анализа Российской академии наук, Москва, Россия. Он является адъюнкт-профессором системного анализа и моделирования систем в Московском физико-технологическом институте (государственный университет). Его основные области исследований включают компьютерное моделирование, а также моделирование приложений интеллектуальных систем для поддержки принятия решений. Он член совета директоров Международного общества по управлению в чрезвычайных ситуациях (TIEMS). Он является членом редакционных коллегий различных научных журналов в области моделирования и эмулирования, а также различных международных рабочих групп. С 2003 года он является членом постоянной группы по контролю информационной безопасности Всемирной федерации ученых. [britkov@gmail.com](mailto:britkov@gmail.com)

Жак Бус (Jacques Bus)

Жак Бус (Jacques Bus) независимый консультант компании *Digitrust.EU*, работающей в области доверия и безопасности информационных и коммуникационных технологий (ИКТ) и научный сотрудник Университета Люксембурга. После 12 лет исследований в области математики он сосредоточился на исследованиях в сфере управления, более 20 лет работает в программе Европейского союза по исследованиям ИКТ, их них последние шесть лет он работает начальником отдела по доверию и безопасности ИКТ. Он является членом постоянной группы по контролю информационной безопасности Всемирной федерации ученых. Он публикует материалы и выступает по вопросам доверия, безопасности, конфиденциальности и управления идентификацией. [http://www.digitrust.eu](http://www.digitrust.eu/" \t "_blank)

Аксель Лехман (Axel Lehmann)

Аксель Лехман (Axel Lehmann) профессор кафедры информатики в Университете вооруженных сил, в Мюнхене, где он занимается моделированием и эмуляцией. Он также председатель университетского Института интеллектуальных систем (ИТИС). Основные направления его исследований лежат в диапазоне от компьютерного моделирования и эмуляции, применения интеллектуальных систем для диагностики и принятия решений, для разработки инновационных компьютерных архитектур. Он бывший президент Международного Общества моделирования и эмуляции, член немецкого общества информатики, член редакционных коллегий различных научных журналов в области моделирования и эмуляции, и член международных рабочих групп и комитетов оценки, например, Европейского союза. Член PMP WFS с 2001 года. [axel.lehmann@unibw.de](mailto:axel.lehmann@unibw.de)

Хамадун Туре (Hamadoun I. Touré)

**Д-р Хамадун И. Туре,** Генеральный секретарь Международного союза электросвязи (МСЭ) с января 2007 года, в октябре 2010 года на Полномочной конференции МСЭ в Гвадалахаре, Мексика. он был переизбран на второй срок. С 1998 по 2006 год он занимал должность директора бюро развития электросвязи МСЭ (БРЭ), и имеет большой опыт работы как в государственном, так и в частном секторах. Родился в 1953 году, д-р Туре имеет степень магистра по электротехнике Ленинградского электротехнического института связи (ЛЭИС, СССР) и степень доктора философии (PhD) Московского технического университета связи и информатики (МТУСИ, Россия). Он стремится превратить МСЭ в инновационную, перспективную организацию, способную решать проблемы, возникающие в стремительно изменяющейся среде ИКТ, и продолжает вести Союз к выполнению резолюций Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО) и достижению Целей Развития Тысячелетия (ЦРТ). [hamadoun.toure@itu.int](mailto:hamadoun.toure@itu.int)

Виталий Цыгичко (Vitali Tsygichko)

Полковник российской армии в отставке, является действительным членом Российской академии естественных наук, а с 1985 г. главным научным сотрудником Института системного анализа Российской академии наук (ИСА РАН). В настоящее время работает экспертом Российского Министерства иностранных дел по проблемам информационной безопасности. С 1967 года он служил в Центральном научно-исследовательском институте Министерства обороны, работая над математическим моделированием военных операций. В 19881991 годах он возглавлял автономный Центр исследований проблем национальной безопасности. Диапазон научных интересов д-ра Цыгичко охватывает методологические и методические задачи моделирования социально-экономических процессов; теорию принятия решений; прикладной системный анализ, теорию и методики социально-экономического прогнозирования, обеспечения национальной безопасности и стратегической стабильности, проблемы информационной безопасности и геополитические проблемы. Он является автором более 200 статей и восьми книг. Он постоянный автор в таких журналах, как "Военная мысль", "Военный бюллетень", "Независимое военное обозрение", а также ряда зарубежных изданий. Он является выпускником Рязанского артиллерийского военного училища, Военной академии им. Дзержинского, и имеет ученую степень доктора технических наук и ученое звание профессора. [vtsygichko@inbox.ru](mailto:vtsygichko@inbox.ru" \t "_blank)

Хеннинг Вегенер (Henning Wegener)

Хеннинг Вегенер (Henning Wegener) бывший посол Германии. Он был послом по вопросам разоружения в Женеве (19811986 годы), помощником Генерального секретаря НАТО по политическим вопросам в (19861991 годы), а затем послом в Испании. В 20012009 годах посол Вегенер был председателем Постоянный Группа мониторинга по информационной безопасности Всемирной федерация ученых, и в настоящее время является ее сопредседателем. Его работа была отмечена в публикациях в области внешней политики и политики безопасности, в том числе кибербезопасности. Среди других званий, г-н Вегенер имеет степень доктора юридических наук Йельской школы права. [henningwegener@hotmail.com](mailto:henningwegener@hotmail.com)

Джоди Р. Вестбай (Jody R. Westby)

Джоди Р. Вестбай (Jody R. Westby) генеральный директор ООО "Глобальные киберриски", расположенного в Вашингтоне, округ Колумбия, она также является почетным ассоциированным членом Киберлаборатории Карнеги-Меллона. Г-жа Вестбай предоставляет консалтинговые и юридические услуги клиентам из государственного и частного сектора по всему миру в таких областях, как конфиденциальность, безопасность, киберпреступность, защиты важнейшей инфраструктуры и экономический шпионаж. Она является председателем Комитета по конфиденциальности и компьютерной преступности (раздел закона о науке и технологиях) Американской ассоциации адвокатов (ABA) и представляет ABA в Национальной конференции юристов и ученых. Г-жа Вестбай была членом Группы экспертов высокого уровня при Генеральном секретаре МСЭ и руководила разработкой *Инструментария МСЭ для законодательства по киберпреступности*. Она является сопредседателем Постоянной группы по мониторингу информационной безопасности Всемирной федерации ученых. Г-жа Вестбай является соавтором и редактором четырех книг по международной киберпреступности, кибербезопасности и неприкосновенности частной жизни, она опубликовала множество статей. Она выступает на глобальном уровне на эти темы.[westby@globalcyberrisk.com](mailto:westby@globalcyberrisk.com" \t "_blank)

Предисловие

В мире 2011 года мы будем пользоваться преимуществами беспроводного глобального информационного общества, но вместе с этими преимуществами приходит угроза кибератак, которые могут происходить в любом месте, в любое время, в мгновение ока, причиняя огромный ущерб. Этот потенциальный ущерб растет по экспоненте за счет связи информационных и коммуникационных технологий (ИКТ) с жизненно важными национальными инфраструктурами.

Для того чтобы остановить эту растущую угрозу мы должны действовать уже сейчас.

На Всемирной встрече на высшем уровне по информационному обществу (ВВУИО) мировые лидеры и правительства доверили Международному союзу электросвязи (МСЭ) решение задачи по координации механизма создания доверия и безопасности при использовании ИКТ. С того времени Генеральный секретарь Хамадун И. Туре начал Глобальную программу кибербезопасности (ГПК), и МСЭ активно действует, стремясь к выполнению этого поручения посредством ряда инициатив. Помимо прочего, МСЭ все еще сильно обеспокоен вопросами киберугроз в его Государствах Членах.

Всемирная федерация ученых (WFS) способствует международному сотрудничеству в области науки и технологии среди ученых и исследователей всех частей мира. Она стремится к продвижению свободного обмена информацией, при котором каждый сможет пользоваться достижениями научного прогресса. В 2009 году Постоянная группа по мониторингу (PMP) информационной безопасности Федерации WFS сформировала проект Декларации Эриче о принципах киберстабильности и кибермира, которая призывает к согласованным международным действиям для гарантий того, что сети информационные и системы будут оставаться устойчивыми, надежными, доступными и проверенными. Декларация была одобрена Пленумом WFS по случаю 42-го собрания Международных семинаров по чрезвычайным ситуациям планетарного масштаба в Эриче, Сицилия 20 августа 2009 года, и была разослана всем Государствам  Членам МСЭ.

Сотрудничество между МСЭ и членами научного и технологического сообщества имеет важнейшее значение для достижения общей цели обеспечения кибермира, Мы не можем эффективно противостоять угрозе кибервойн без участия тех, кто обладает знаниями и пониманием технологий, которые изменяют глобальный пейзаж.

Этот документ присоединяет свой голос к голосу сообщества. Он представляет собой необходимый шаг в процессе создания международного сотрудничества для решения этих проблем. Мы признательны за возможность высказать все наши взгляды на этот важнейший вопрос.

|  |  |
| --- | --- |
| Д-р Хамадун И. Туре  Генеральный секретарь  Международный союз электросвязи | Профессор, д-р Антонино Дзикики  Президент  Всемирная федерация ученых |

# 1 Введение

**Джоди Р. Вестбай (Jody R. Westby)**

Цель данной публикации – продвижение концепции глобального кибермира путем:

• Изучения того, как ИКТ является основой повседневной жизни;

• Оценки современных киберугроз и их тенденции;

• Анализа последствий киберпреступности и киберконфликтов;

• Оценки пригодности существующих правовых рамок;

• Определения концепции кибермира и установления ее в качестве основного руководящего принципа мирного существования в киберпространстве; и

• Планирования дальнейшего пути.

Интернет – центральная нервная система общества. Учтите, что все ключевые сектора инфраструктуры зависят от ИКТ. Они управляются системами диспетчерского контроля и сбора данных (SCADA) и другими сложными процессами информационных технологий (IT), которые каким-либо способом соединены с интернетом. Например, больницы и медицинские центры используют ИКТ для всего – от оказания экстренной помощи до систем жизнеобеспечения. Нефтяной, газовый и транспортный сектора создают сложные системы обработки и навигации, которые полностью компьютеризованы, а финансовые компании работают с системами электронных платежей и электронной обработки данных. Правительства зависят от ИКТ при предоставлении услуг, управлении работой в разных географических регионах, поддержании общественной безопасности и защите своих территорий. Предприятия полагаются на компьютерные системы, которые управляют цепочками поставок, взаимоотношениями с клиентами, финансовыми потоками, а также выполняют функции производства. А системы связи и сети энергоснабжения являются "суперкритической" инфраструктурой, от которой зависят все остальные.

Интернет сегодня также неразрывно вплетен в повседневную работу и жизнь людей. Будь то работа, учеба или игры, во всем участвуют ИКТ. Интернет дает возможность распространения знаний и информации на уровне, не имеющем аналогов в мировой истории. Возможности социальных сетей соединяют народы и влияют на них такими способами, которые полностью отделены или неподконтрольны их правительствам. Это дало возможность расширения прав и возможностей личности, расширения собственного "я", и распространения необычных идей посредством механизма, который практически не видит границ, а также слеп к дипломатическим или политическим соображениям. Сегодня, человек может быстро влиять на восприятие, ценности, идеи и предубеждения других людей лишь в силу своей способности создавать контент и распространять его в глобальном масштабе.

Распространенность интернета, однако, также породила преступную деятельность и создала новые возможности для сбора разведывательных данных и возникновения конфликтов. Уязвимости операционных систем, программного обеспечения и настроек безопасности позволяют выполнять действия, которые угрожают основным услугам для гражданского населения, упрощают экономический шпионаж и влияют на действия правительства. Вирусы, черви, распределенные атаки класса отказ в обслуживании (DDoS), кражи персональных данных, спам и мошенничество подрывают надежность ИКТ и способность к действию общества и государства.

Эффективные программы безопасности повысят устойчивость систем и помогут обнаруживать, и предотвращать такие действия, а также смягчать их последствия. Технологические улучшения и инновации помогут блокировать и отслеживать атаки, а гармонизированные законы о киберпреступности будут способствовать расследованию и уголовному преследованию киберпреступников. В каждой из этих областей предстоит сделать много работы, но наиболее опасна и потенциально разрушительна такая проблема, когда государства используют тактику разжигания киберконфликтов[[1]](#footnote-1). В настоящее время известно множество примеров того, как политические и военные конфликты распространяются в киберпространстве, заметно подрывая доверие к ИКТ и представляя серьезную опасность. Некоторые из этих случаев описаны в последующих главах этой публикации.

До появления информационного общества власть и лидеры, как правило, поддерживались теми, кто имел политическую власть, военное превосходство, и экономическое господство. Государства и международные организации диктовали социальные нормы и ценности, и вооруженные конфликты урегулировались по законам и договорам, основанным на территориальной целостности и обороноспособности на земле, в воздухе и на море. Однако сегодня интернет резко изменил этот баланс власти. Ничто не иллюстрирует эту точку зрения лучше, чем история самого интернета.

События в мире могут быть важными мотиваторами. После Второй мировой войны Америка столкнулась с противниками нового вида: Холодной войной, коммунизмом и угрозой ядерных ударов. В ответ на озабоченность по поводу советского научного превосходства после запуска первого искусственного спутника Земли, президент Эйзенхауэр основал Агентство перспективных исследований и проектов Министерства обороны США (ARPA), в настоящее время DARPA, для координации всех технических исследований США[[2]](#footnote-2). Для руководства программами компьютерных исследований ARPA был нанят Дж. С. Р Ликлидер (J.C.R. Licklider), ранее работавший в Масачуссетском технологическом институте (MIT). Несколькими месяцами ранее он опубликовал серию записок с обсуждением "Галактической сети" из соединенных между собой компьютеров, которая позволяет иметь общий доступ к программам и файлам. Позже Винт Серф (Vint Cerf), Боб Кан (Bob Kahn) и некоторые другие "отцы интернета" отметили, что "по своему духу концепция был очень похож на интернет сегодняшнего дня"[[3]](#footnote-3).

Примерно в это же время военно-воздушные силы забеспокоились относительно своей способности поддерживать командование и управление операциями после ядерной атаки, и поручили RAND провести исследование жизнестойкости военной сети, которая могла бы обеспечить "минимально необходимые коммуникации"[[4]](#footnote-4). Работа RAND (19621965 годов) завершилась докладом Поля Барана описывающим, как с этой задачей может справиться компьютерная сеть с коммутацией пакетов[[5]](#footnote-5). Одновременно (и без ведома группы RAND) три инженера Массачусетского Технологического Института рассматривали концепцию объединенных в сеть компьютеров и коммутацию пакетов[[6]](#footnote-6). В конце 1966 года один из инженеров Массачусетского технологического института, Лоуренс Робертс, перебрался в DARPA ",для того чтобы разработать концепцию компьютерной сети"[[7]](#footnote-7).

Оставшаяся часть – это всем известная история. В 1971 году сеть ARPANET, как первоначально назывался интернет, имела 23 узла, соединяющих правительственные исследовательские центры и университеты США. К 1981 году эта сеть уже называлась интернетом, а к 1991 году стала реальностью Всемирная паутина (разработанная сэром Тимоти Бернер-Ли[[8]](#footnote-8) в Европейской организацией по ядерным исследованиям (также известной как ЦЕРН). Сочетание интернета и веба идеально для коммерческого использования, но корпорациям был заблокирован доступ к магистрали через сеть NSFNET Национального научного фонда (NSF).

В 1995 году NSF сдал свои позиции и превратился в магистраль доступа к интернет из четырех коммерческих компаний, и к 1996 году интернет насчитывал около 10 миллионов хостов, и интернет распространился по всему миру. В течение трех десятилетий, интернет вырос "из концепции холодной войны по управлению осколками мира постъядерного общества в информационную супермагистраль"[[9]](#footnote-9). Вместе интернет и World Wide Web пронизывает экономику и общества на всех уровнях и вершат социальные преобразования, которые были немыслимы 20 лет назад. Сегодня в мире насчитывается почти два миллиарда пользователей интернета, без каких-либо географических границ. Управление интернетом сегодня охватывает как технические проблемы, так и вопросы государственной политики и в нем принимают участие все заинтересованные стороны, а также соответствующие межправительственные и международные организации

Ирония заключается в том, что это детище эры Холодной войны в сочетании с интернационализации науки, которая привела к появлению интернета, в настоящее время представляет собой одну из наиболее важных проблем глобального мира. Несмотря на то, что при анализе национальных и экономических интересов в области безопасности геополитические[[10]](#footnote-10) факторы по-прежнему требуют к себе большого внимания, интернет изменил традиционный анализ внешней политики. Геокиберразмеры все больше влияют на поведение государств, и геополитические блоки ускоряют появление новой парадигмы

Проблема сохранения "минимально необходимых коммуникаций" перестает быть вопросом только США: это теперь вопрос о том, как *все* страны мира могут поддерживать геокиберстабильность и гарантировать, что их важнейшие инфраструктуры не смогут быть использованы в качестве оружия против невинных и беззащитных граждан, принося ненужные страдания и разрушения.

Автор определяет "геокибер", как отношения между интернетом, географией, демографией, экономикой и политикой страны, и ее внешней политикой. "Геокиберстабильность" определяется, как способность всех стран использовать интернет для получения экономических, политических и демографических выгод, при условии отказа от действий, которые могли бы причинить излишние страдания и разрушения[[11]](#footnote-11).

Сегодня весь мир сталкивается с новыми угрозами, возникающими из интернета, и способность каждого государства охранять свои коммуникации, управление, контроль и возможности компьютеров (С4) противостоять атакам террористов, организованных в преступные группировки, и других государств стала неопределенной. ИКТ ставит перед странами беспрецедентные проблемы власти национальной и экономической безопасности. Физические лица могут теперь бросить вызов власти и осуществить асимметричные атаки, которые способны парализовать всю инфраструктуру и оборвать коммуникации, и теперь слабые системы могут угрожать безопасности из величайших наций.

Киберконфликт может иметь опасные для жизни последствия, когда рушатся важные информационные инфраструктуры. Он также может привести к выполнению действий над информацией, которые посягают на международные права человека, провоцируют насилие и приводят к серьезным экономическим потерям. Риски для отдельных лиц и государства огромны  и выпадают из существующих правовых рамок, которые мало пригодны для кибернетической эры

Необходимость имеет экстренную природу. Быстрые темпы, с которыми страны создают киберуправление и усиливают свой военный потенциал для борьбы с киберконфликтами, должны быть сбалансированы соглашением между государствами, которое признавало бы новый уровень "минимально необходимых коммуникаций", защищенных от конфликта. Такие действия предотвратят ненужные разрушения и страдания тех, кто участвует в конфликте, и защитят не вовлеченные в конфликт страны. Такой уровень геокиберстабильности жизненно необходим, чтобы преимущества интернет были бы недоступными для разрушительных сил технологии.

Логической отправной точкой являются многонациональные организации. Они должны начинать с определения минимального уровня стабильности, инфраструктуры и коммуникаций, необходимого для защиты мирных граждан и поддержания основных общества, а также обеспечить это посредством дипломатических соглашений и законодательных правил. Для этого потребуется участие широкого круга заинтересованных сторон, в том числе граждан, промышленности, гражданского общества, научных кругов, юристов, экспертов в области политики, экстренных служб и правоохранительных органов. Таким образом, ИКТ и интернет смогут создать положительную международную основу для сотрудничества между странами и привести к лучшему пониманию и принятию различных культурных и общественных ценностей во всем мире.

Эта книга основана на концепции кибермира как целевого принципа существования в киберпространстве. Следовательно, всем странам следует стремиться к кибермиру. Преимущества кибермира намного перевешивают разрушительные последствия киберконфликтов.

Данная публикация, написанная в соавторстве с Генеральным секретарем Международного союза электросвязи Хамадуном И. Туре и членами постоянной группы по мониторингу информационной безопасности Всемирной федерации ученых, предназначена служить для всех заинтересованных сторон призывом к действию по объединению усилий в деле обеспечения минимального уровня стабильности в интернете и их инфраструктурах и дальнейшего развития концепции глобального кибермира.

# 2 Киберпространство и угроза кибервойны

**Хамадун И. Туре (Hamadoun I. Touré)**

Информационные и коммуникационные технологии (ИКТ) становятся неотъемлемой частью ежедневной жизни для множества людей в мире. Цифровая связь, сети и системы предоставляют жизненно важные ресурсы и незаменимую инфраструктуру для всего мирового сообщества, необходимыми вещами, без которых многие народы не могли бы развиваться или даже выжить. Эти структуры и системы представляю собой новую сферу, и вместе с ними проходят новые задачи по сохранению мира и стабильности. Не имея механизмов гарантии мира, города и сообщества мира будут уязвимыми для атак беспрецедентного и бесконечного разнообразия. Такая атака может начаться без предупреждения. Внезапно компьютеры и сотовые телефоны прекратят работу, экраны банкоматов и автоматических касс выдачи наличных будут безучастно смотреть на потребителей, управление воздушным движением, системы управления трафиком на железных и автомобильных дорогах покинут скоростные магистрали, мосты и водные пути погрузятся в хаос, а скоропортящиеся грузы застрянут вдали от голодающего населения. Потеряв энергоснабжение больницы, дома, торговые центры, все сообщество целиком погрузятся во тьму. Правительственные организации не смогут оценить ущерб, связаться с остальным миром, рассказать о кризисе или защитить своих уязвимых граждан от последующих атак. Это неразрешимое бедственное положение сообщества, парализованного из-за мгновенной потери цифровых сетей. Это возможные разрушения, вызванные новым видом войны,  "кибервойны".

Новая область: Киберпространство, безопасность и способы войны

Угроза кибервойны сегодня вырисовывается больше, чем когда-либо. Сегодня, технологические достижения и растущая цифровая инфраструктура связывают все население со сложными, переплетающимися системами. Спрос на интернет и цифровую связь призывает к еще большей интеграции ИКТ в продукты, которые ранее работали без него, например, автомобили, здания и даже системы управления огромной мощности и транспортные сети. Энергоснабжение, транспортные системы, военные службы и логистика, практически все современные службы зависят от использования ИКТ и стабильности киберпространства. "Киберпространство" это физическая и концептуальная реальность, в которой существуют эти системы. Следовательно, "кибервойна" в широком смысле может пониматься как война, ведущаяся в киберпространстве, с использованием ИКТ и нацеленная на ИКТ[[12]](#footnote-12). Быстро растущая зависимость от интеллектуальных энергосистем и других систем управления и контроля на базе интернет-технологий приводит к тому, что главные ресурсы энергии, транспорта и обороны оказываются достижимыми для тех, кто стремится к тому, чтобы посеять хаос в правительстве и гражданском населении[[13]](#footnote-13). Таким образом, усиленные инфраструктуры кибербезопасности и защиты критической информации теперь становятся важнейшими элементами безопасности каждой страны и благосостояния экономики

С ростом глобальных надежда на ИКТ растет и уязвимость к атакам критических инфраструктур в киберпространстве. Несмотря на то, что точные контуры "кибервойны" все еще не определены, значительные атаки против информационных инфраструктур и служб интернета в последнее десятилетие позволяют ощутить возможную форму и область конфликта в киберпространстве. Атаки в Грузии[[14]](#footnote-14), Эстонии[[15]](#footnote-15), Южной Корее и США[[16]](#footnote-16) были связаны с боевыми действиями кибервойны. Множественные отключения в Бразилии были связаны с кибератаками и, в 2008 году хакеры взломали веб-сайт Правительства и контролировали его в течение недели[[17]](#footnote-17). Отключения в Бразилии иллюстрируют возможный объем нарождающихся видов кибератак: отчеты о них подобны кадрам научно-фантастического фильма, с подземными поездами, светофорами и плотиной второй крупнейшей в мире гидроэлектростанции *Itaipu*, разрушение которой приводит к ужасной остановке, затронувшей более 60 миллионов человек[[18]](#footnote-18).

Кибервойна может затронуть также и частный сектор. Гиганты веб-сервиса такие как *Google*[[19]](#footnote-19) и *Twitter*[[20]](#footnote-20) уже испытании атаки в 2009 году, а еще раньше – в 2000 году, атаки типа "отказ в обслуживании" были направлены на такие известные компании как *CNN, Ebay* и *Amazon*[[21]](#footnote-21)*.* В результате некоторые службы были недоступны в течение нескольких часов или даже дней. Хакеры нацелились на системы управления аэропортом, отключив такое важнейшее оборудование, как телефонные линии и взлетно-посадочные огни[[22]](#footnote-22). По некоторым расчетам за последние три года более шести стран испытали на себе кибератаки, и только в первые месяцы 2010 года были атакованы, как минимум, 34 частные компании[[23]](#footnote-23). Несмотря на то что эти проблемы безопасности серьезны, еще не слишком поздно предотвратить возможные катастрофические сценарии, путем создания безопасных продуктов, методов и стандартов в тесном международном сотрудничестве[[24]](#footnote-24). Задачи повышения безопасности интернета и защиты ИКТ от разрушения и уничтожения должны стать приоритетными, если мы собираемся защитить гражданское население, гарантировать эффективную работу базовых структур и обеспечить непрерывную разработку новых услуг.

Кибервойна как угроза для национальной инфраструктуры

Понятие кибервойны охватывает опасности не только для военных средств и систем, но также и для жизненно важной общественной инфраструктуры, включая интеллектуальные энергосистемы, сети диспетчерского управления и сбора данных (SCADA), которые позволяют им работать и осуществлять самозащиту. Используя различные среды (киберпространство и работающие в нем ИКТ), противник может развернуть вооружение и использовать его в оборонительно-наступательный конфликт также как и традиционное оружие. Тактика военных действий в кибервойне обычно предполагает сбор данных или внедрение в компьютеризованную систему с целью повреждения важнейших ее компонентов[[25]](#footnote-25). Среди возможного оружия для кибервойны есть компьютерные вирусы и черви, для сбора киберданных используются станции создания помех, взломанные контрафактные компьютерные программы, импульсное, электромагнитное оружие, средства разведки в компьютерах и сетях, а также встроенные троянские бомбы замедленного действия.

Все большая надежда на интеллектуальные энергосистемы делает системы электроснабжения многих стран особенно уязвимыми к атакам. Интеллектуальные энергосистемы это цифровые системы, которые связывают распределительные сети с центральной сетью контроля, которая часто называется сетью SCADA. Сети SCADA собирают информацию об использовании и подаче энергии, тогда как интеллектуальные энергосистемы создают цифровой канал, для того чтобы передавать эту информацию между потребителями и поставщиками[[26]](#footnote-26). Эти технологии сегодня используются для самых разных процессов и систем, включая системы водоснабжения, газопроводы, линии и распределительные сети электропередач, системы ветровой энергетики, системы массовых коммуникаций, изготовление, производство, системы общественного транспорта, системы экологического контроля, управления воздушным движением и светофорами[[27]](#footnote-27). Все больше и больше поставщиков присоединяют интеллектуальные энергосистемы к интернету, для того чтобы иметь удаленный доступ и расширение функциональных возможностей.

При подключении сети предоставляют существенные преимущества, например сокращение потерь энергии и более быструю связь клиентов с поставщиками, они также централизуют данные и управление огромной энергосистемы в сети, которая имеет несколько точек доступа. Имея больше конечных точек и более взаимосвязанную сеть, интеллектуальные энергосистемы и сети SCADA дают злоумышленникам множество возможностей для проникновения в них[[28]](#footnote-28). Например, интеллектуальный измеритель (счетчик электроэнергии, подключенный к сети) может быть довольно легко взломан и заражен вирусами, и затем он может быть использован для распространения червя на другие измерители и, в конечном итоге, привести к замыканию или отключению электрических сетей[[29]](#footnote-29). Хотя многие фирмы

стремятся обезопасить свои сети путем изоляции центров управления от других сетей (метод называется "сокращение воздуха"), попытки полностью изолировать отдельные компоненты часто терпят неудачу, причем зачастую незаметно для администратора системы[[30]](#footnote-30). Логические бомбы, которые являются еще одним способом для нападающих, могут нарушить или даже уничтожить интеллектуальную энергосистему, хакеры могут проникнуть в сеть, для того чтобы скрыть в ней вредоносные программы, ожидающие активации этих бомб в более позднее время с целью скоординированного нападения или создания ограниченных перебоев электроснабжения[[31]](#footnote-31). Такие бомбы создают дополнительные проблемы безопасности, поскольку они могут быть взорваны случайно или другим хакером, который обнаружит их позднее[[32]](#footnote-32).

Уже сейчас страны, которые вложили средства и сообщают о попытках атак и покушений, число которых достигает тысяч в день[[33]](#footnote-33). По некоторым оценкам, кибератаки являются наибольшей угрозой для данного поколения национальных энергосистем[[34]](#footnote-34). Дистанционная атака вполне может быть нацелена на физическую инфраструктуру, например, генераторы и трансформаторы, заставляя их, в сущности, выполнять действия по самоуничтожению[[35]](#footnote-35). Такая атака, скорее всего, будет иметь дальние последствия, так как энергетические компании обычно не держат на складах дорогостоящие запасные части, и их изготовление и поставка может занять несколько месяцев[[36]](#footnote-36). Атака на интеллектуальную энергосистему не только оставит потребителей без власти, но она может также причинить значительный финансовый ущерб. Генераторы энергии могут приносить многомиллионные доходы в

долларовом исчислении, и общий объем инвестиций в интеллектуальные энергосистемы для некоторых стран достигает десятков миллиардов[[37]](#footnote-37).

Помимо возможности больших физических разрушений и непосредственных финансовых потерь, угроза будущих кибератак подрывает доверие к существующим и новым технологиям, таким как "умные" электросети и, в свою очередь, в надежности электронных, финансовых и медицинских ресурсов. Даже одна эта потеря доверия может привести к огромным социальным и экономическим потрясениям[[38]](#footnote-38). Расширение использования умных электросетей вместе с ядерными реакторами (и ядерным оружием) создает еще большие риски и потенциальный ущерб. Кроме традиционных атаки и стратегии обороны, кибервойн может также использовать атаки на внутренние системы предприятия или государства, для того чтобы временно отвлечь[[39]](#footnote-39) ресурсы или воспрепятствовать их работе, в отличие от непосредственно повреждая. страна может выбрать этот вид кибератаки, если, например, он хочет отключить союзных поддержку целевого противника достаточно долго для достижения конкретной цели., чтобы отключить союзных поддержку целевых противника достаточно долго для достижения конкретной цели[[40]](#footnote-40).

Уникальные возможности и влияние кибервойн

Хотя кибервойна может напоминать традиционные методы ведения войны в некотором роде, уникальных характеристик киберпространство привносят в них новые и непредвиденные аспекты. Поскольку системы в киберпространстве связаны компьютерами и сетями связи, разрушения, вызванные ИКТ атаками, значительно превышают отказ одной системе, и зачастую выходит за пределы национальных границ. Многие процессы передачи данных затрагивают несколько стран, и многие интернет услуги основаны на услугах, получаемых из-за границы, например, хост провайдеры могут предлагать веб-пространство для размещения домашней страницы в аренду в одной стране, используя оборудование, находящееся в другой стране. Даже короткие перерывы в предоставлении услуг могут привести к огромным финансовым потерям для электронной коммерции. Гражданские сети связи являются не только системами, уязвимыми для атаки, зависимость от ИКТ представляет большой риск и для военной связи тоже. В отличие от более традиционных бойцов, киберпреступникам нет необходимости лично присутствовать там, куда осуществляется нападение, или даже там, откуда оно, как представляется, исходят. Кроме того, во время выполнения атаки, для того чтобы скрыть свою личность, преступники могут использовать анонимные коммуникации и технологии шифрования[[41]](#footnote-41).

Кроме того, для автоматизации атак используются программные средства, которые свободно доступны в интернете. С использованием такого программного обеспечения и предустановленных атак, один преступник в один день и с одного компьютера может атаковать тысячи компьютерных систем. Если у преступника есть доступ к нескольким компьютерам, например посредством ботнета(ов), он может еще больше увеличить масштаб нападения. Например, из анализа атак на правительственные веб-сайты в Эстонии можно предположить, что они были совершены путем объединения в "ботнет" тысячи компьютеров или с использованием группы зараженных компьютеров, программы на которых работали под управлением извне[[42]](#footnote-42). Ботнеты также усложняют задачу отслеживания преступника, так как изначальные следы ведут только к другим участникам ботнета. Современный анализ показывает, что до четверти всех компьютеров, подключенных к интернету, может быть заражены программами, которые делают их составной частью ботнета.

Программы также упрощают атаки, что позволяет совершать кибератаки менее опытным пользователям компьютеров или менее развитым военным подразделениям. Кроме того, атаки с использованием ИКТ, как правило, дешевле, чем традиционные военные операции и их могут осуществлять даже малые государства. Теперь, даже государство с исторически более слабым военным потенциалом способно значительно повредить важнейшие инфраструктуры посредством кибератак. Эта возможность асимметричных действий превращает кибервойну в привлекательную стратегию боевых действий со сценарием(ями), обратным(и) сюжету борьбы Давида против Голиафа. Боязнь кибервойны, подкрепленная фактами (хотя и ограниченными в числе) возникновения кибератак подрывает доверие общественности к ИКТ. Таким образом, потенциальный психологический эффект от возникновения киберконфликта может привести к широкомасштабному снижению эффективного использования новых технологий и создавать препятствия для прогресса во многих секторах.

# 3 Зависимость и доверие в обществе

## 3.1 Зависимость современных обществ от ИКТ и интернета

**Жак Бус (Jacques Bus)**

Компьютеры и информационные технологии существуют со второй половины прошлого века, а интернет появился всего лишь 38 лет назад как часть сети связи в проекте ARPA (DARPA). Однако только в последние 15 лет, благодаря изобретению Всемирной паутины (для удобства в данном документе комбинацию интернета и сети мы будем называть "интернетом"), Интернет позволил экономики и социальной жизни развиваться с ошеломительной скоростью. В настоящее время мы можем наслаждаться общением в социальных сетях в любое время и в любом месте; у нас есть практически неограниченный доступ к информации; мы можем вступать в дискуссии и общаться с людьми со всего мира; и мы выбираем и заказываем услуги и товары, сидя дома в уютном кресле в любое удобное для нас время.

Согласно оценкам МСЭ за 2009 год, 25,9% населения мира имеет подключение к интернету (что составляет примерно 1,8 миллиарда человек). Люди проводят в интернете в два раза больше времени, чем за просмотром телевизора. По всему миру насчитывается 4,6 миллиарда абонентов сотовой связи, что равно 67% мирового населения. Только в одной сети Facebook в июле 2010 года было зарегистрировано более 500 миллионов активных пользователей, а Facebook, Myspace и Twitter вместе в июле 2010 года привлекли 220 миллионов активных посетителей. Одним из важных изменений в мировом масштабе стало превращение мобильного телефона в интернет телефон, который заменил собой ПК в роли предпочтительного устройства для подключения к интернету. 9,5% мирового населения уже имеет доступ к широкополосной подвижной связи.

Хотя интернет уже серьезным образом и действительно в мировом масштабе изменил современное общество, еще многое предстоит сделать. Во многих публикациях[[43]](#footnote-43) мы читаем сценарии будущего, описывающие как может выглядеть мир через 25 лет. Обычным явлением будут удостоверения личности, используемые для доступа к общественному транспорту, медицинским картам, доступа к правительственным и сетевым услугам. Социальные сети будут расширены, и для них будут найдены новые, более эффективные и впечатляющие применения. Технологии передачи данных создадут новые информационные услуги, которые помогут исследователям эффективнее проводить исследования, путешественникам получать больше удовольствия от путешествий, гражданам понимать правила управления и побудительные причины политических решений и т. д. А при помощи агентских программ и политических процессов можно будет устранить большинство административных препятствий, например, при договоренности о встрече, подготовке к встрече и проверке соответствие полномочий сфере деятельности.

Социальная революция на основе ИКТ приведет к важным изменениям в равновесии сил как на национальном уровне, где граждане получат широкий доступ к информации о политических процессах, которую можно использовать в демократических процессах, так и на международном уровне. Доступ в интернет дает гражданам возможность иметь больше влияния на экономическую и политическую жизнь и понимать ситуации и образ жизни других народов. Мы видели, как президент США Обама использовал социальные сети в своей избирательной кампании, и можем ожидать, что в будущем похожие действия будут все чаще использоваться для поддержки создания правил правительствами.

ИКТ также позволяют международным компаниям организовать себя так, чтобы наилучшим образом воспользоваться возможностями по всему миру. Все это может дать мощный импульс экономическому развитию и росту по всему миру, а особенно в странах с малыми затратами на производство. Мы уже видим, как крупные развивающиеся страны используют эти преимущества и становятся важными игроками на экономической и политической арене.

Однако как и во всякой революции в истории человечества, наряду с возможностями и преимуществами всегда существует обратная сторона.

Информационно-коммуникационные инфраструктуры и услуги стали очень важной частью нашей экономики. Они крайне уязвимы, так как почти каждый день приходят сообщения о множестве атак. Большая часть наших важнейших инфраструктур, например, энергетические, водные, транспортные и финансовые системы в области связи и управления в значительной степени зависят от ИКТ. Поэтому высок уровень возможности происшествий или преднамеренных нападений на такие важные инфраструктуры, которые потенциально могут привести к хаосу и колоссальным экономическим потерям. Это включает в себя вторжение и атаки на системы и базы данных национальных агентств безопасности.

Такая уязвимость нашей социальной инфраструктуры ИКТ делает ее удобной мишенью для "кибервойн" или "кибертерроризма", что создает угрозу геополитической стабильности. Умышленная организация атак на важные системы общества одного государства при одобрении, поддержке или управлении со стороны другого государства иногда называется "кибервойной". Однако следует отметить, что слово "война" в данном контексте может создать недопонимание, так как в большинстве случаев это не соответствует общему пониманию людей о войне: долгосрочное разрушение физической инфраструктуры и большие людские потери.

За последние несколько лет произошло несколько атак, для описания которых использовался термин "кибервойна"; например, в Эстонии,[[44]](#footnote-44) Грузии, Южной Корее, США. Иногда она начинается с любительской психологической "войны" с пропагандистскими целями, которая на втором этапе включает атаки, осуществляемые специалистами по кибератакам (преступниками или кем-то еще), в полномасштабной кампании посредством запуска через ботнеты DDoS-атак на социальную и экономическую инфраструктуру. В других случаях кибератаки проводятся непосредственно до или во время динамических военных действий. Вплоть до настоящего времени разрушения, вызванные кибератаками, были в основном ограниченными, и деятельность могла быть восстановлена спустя несколько дней, и не встречалось упоминания о человеческих жертвах, напрямую обусловленных кибератаками.

Роли, которые государства сыграли в этих конфликтах, в основном не подтверждены. Но это доказывает важность достичь соглашений на международном уровне по поводу ограничений и защиты от кибератак и по международному сотрудничеству с целью установления контроля. Очевидно, что старая доктрина предупреждения в Холодной войне не имеет удобного применения в киберпространстве. Нет полного понимания того, из чего может состоять такое предупреждение и, более важно, очень трудно идентифицировать врага (невозможность установления подлинности и использование агентов доступа).

Давайте оставим в стороне политические дебаты по поводу термина "кибервойна". Нет никакого сомнения в том, что киберпреступность становится весьма серьезной проблемой. Количество злоумышленных и преступных угроз безопасности растет в геометрической прогрессии. Только в 2008 году компания Symantec зарегистрировала 1,6 миллиона угроз, что составило 60% от общего количества зарегистрированных угроз за все время до 2008 года. Более 8 миллионов граждан США стали жертвами кражи идентичности. Средняя стоимость искажения данных в США была оценена в 6,7 миллиона долларов США. А в феврале 2010 года стало известно, что по всему миру 750 000 компьютерных систем компаний были заражены и превращены в ботнеты. Амит Йоран (Amit Yoran), бывший руководитель одного из агентств США, предположил, что компании просто не готовы защищать себя, хотя позднее это было недооценено сектором безопасности США.

Говард Шмидт, (помощник президента США по специальным вопросам и координатор по кибербезопасности), признавая, что существует растущая проблема злонамеренного использования интернета, определяет, тем не менее, четкие приоритеты. Он отвергает термин "кибервойна" как "ужасное понятие". Он не видит победителей в таких условиях и предлагает сконцентрироваться на преступности и шпионаже в онлайновой среде.

Несмотря на разницу во мнениях, существует общее согласие относительно того, что есть причины для беспокойства по поводу безопасности и доверия в интернете. Существующие тенденции говорят о росте опасений и неприятия гражданами нового цифрового мира. Это может иметь колоссальные экономические последствия, если политики и разработчики технологий не смогут справиться с этими негативными социальными аспектами.

В своей речи 21 января 2010 года Государственный секретарь США Хиллари Клинтон подчеркнула важность для всемирного сотрудничества и развития открытого и свободного доступа в интернет. Она сослалась на "Четыре свободы" Рузвельта – свободу слова и вероисповедания, и свободу от нужды и страха – и важное влияние интернета на эти свободы, особенно на свободу слова. Интернет привел к революции в области обмена информацией и социального взаимодействия. Он имеет большой потенциал для увеличения благосостояния любого человека, особенно, когда будет полностью признана "свобода связи". Однако он также привел к росту всемирной преступности и появлению страха, который следует сдерживать.

Политики полностью признали крайнюю важность интернета на всемирной геополитической арене. Они понимают, что граждане ожидают, что правительства гарантируют им безопасность и защиту, в то время как национальные юрисдикция и границы более не дают такого ощущения, как это было раньше. Потребительское право в том виде, как оно применяется в настоящее время во многих странах, также как и надежность товаров и услуг не работают в мире, где потребитель и поставщик принадлежат разным и не сотрудничающим юрисдикциям, а услуги предоставляются по случайным цепочкам субуслуг, используя данные из глобальной сети, распределенной по всему миру.

Мировые лидеры столкнулись с колоссальными и беспрецедентными проблемами. Изменение климата, быстрые изменения во всемирном экономическом балансе сил и энергетической безопасности, например, необходимость политического внимания к всемирной цифровой связи и риски, с нею связанные. Для решения этих проблем нам потребуется крепкое и мудрое всемирное руководство.

В этой ситуации наиболее важно использовать то, что мы узнали из истории об общественном устройстве и ценностях, безопасности, доверии и международных связях. Мы должны использовать всемирное изменение для обмена нашими культурами, общественными ценностями и сильными сторонами и процессами международного сотрудничества так, чтобы их можно было использовать в мире, где признают реальность цифровой связи.

### **Необходимость доверия**

Понятие доверия и его роль в обществе

*"Доверие наполняет повседневную жизнь. Если мы возьмем всего лишь небольшой пример из массы событий, где участвует доверие, мы увидим, что из всех общественных явлений оно, без сомнения, самое необходимое. Но именно это центральное положение создает проблемы для изучения природы доверия – Как вообще можно начать понимать, что собой представляет такая многогранная общественная сила[[45]](#footnote-45)?"*

Доверие и надежность являются понятиями, которые лежат в основе человеческого существования. Мы их используем интуитивно, а их значение постоянно зависит от контекста. Но когда мы переносим эти понятия в цифровую среду, мы легко можем попасть в неприятное положение.

Луманн (Luhmann)[[46]](#footnote-46) объясняет доверие как механизм, уменьшающий сложность и позволяющий людям справиться с высоким уровнем неопределенности и сложности (современной) жизни. Таким образом, доверие расширяет возможности человека, для того чтобы успешно найти общий язык с реальным миром, чья сложность и непредсказуемость гораздо выше, чем мы та, которую мы в состоянии понять. В этом смысле оно является важным механизмом, позволяющим людям жить своей жизнью: общаться, взаимодействовать, совершать экономические сделки и т. д. Оно улучшает жизнь человека, поддерживая его действия, смелость, авантюризм и творчество, и расширяя границы общения человека с другими людьми.

Если рассматривать с другой точки зрения, можно сказать, что доверие – это ожидание благоприятных действий в отношении доверяющей стороны в определенных ситуациях. Как объяснял Хардин (Hardin):[[47]](#footnote-47) "Доверие относится к когнитивной категории вместе со знанием и верой. Сказать Я тебе доверяю – это сказать не больше, чем Я знаю или думаю, что знаю, определенные факты о тебе, которые позволяют мне верить, что ты достоин моего доверия и будешь действовать "благоприятно" даже в непредсказуемых ситуациях".

Доверие – это трехсторонние отношения (*A доверяет B сделать X*). Уровень доверия, которое *A* имеет к *B*, чтобы сделать *X*, играет важную роль в решении *A* принять участие в любой сделке, обмене или общении с *B*. Уменьшая сложность и осознаваемый риск, доверие эффективно упрощает экономическую деятельность, творчество и инновации. Доверие в высшей степени зависит от контекста. Оно зависит от: времени (можно с легкостью потерять доверие к кому-то, но и само понятие со временем изменяется); истории и памяти; места и ситуации; культуры; роли (личности или профессионала); эмоций; и множества других переменных (например, социологических соображений, например, репутации, повторения и рекомендаций).

Из вышесказанного очевидно, что доверие является понятием, которое может быть упрочено в определенной степени в определенной ситуации и между двумя определенными сторонами. Более подробная информация, может быть полученная при помощи других датчиков или в результате общения, может помочь укрепить доверие, как и большую длительность успешных взаимоотношений.

В целом, в данном обсуждении мы можем предположить, что стороны *A* и *B* являются людьми. Это не исключает вероятности того, что эти люди действуют от лица организации или группы людей. Однако на практике многие люди также могут говорить о доверии к другим объектам, например, правительству, компании, системе или услуге, базе данных или информационной услуге (например, документу, техническому блогу), или, может быть, даже к виртуальному объекту, например, программному инструменту. Хардин называет это "доверием к действиям, поведению или достоверности объекта". Оно может быть основано, например, на подотчетности, прозрачности, гарантиях и обязательствах, аудиторских проверках и репутации или знании о намерениях объекта.

Понятие доверия как социального капитала, или "социального доверия", обсуждалось и было разработано Фукуямой (Fukuyama),[[48]](#footnote-48) Путнэмом (Putnam)[[49]](#footnote-49) и другими экспертами. Это статистическое понятие, выражающее мнение людей о надежности их общества во всех аспектах, или точнее, уверенности людей в правительстве, институтах, законах, системе и т. п. в обществе. По-видимому, существует тесная взаимосвязь между высоким уровнем социального доверия и высоким уровнем экономического роста и процветания.

Мы также будем в основном использовать термин "доверие" там, где Хардин сказал бы "уверенность". Однако для дальнейшего обсуждения важно различать доверие между людьми в сетевых цифровых системах и услугах для взаимодействия, и доверие или уверенность человека в объектах или институтах, не принадлежащих к человеческому роду.

Введение цифровой технологии изменило способы общения и взаимодействия между людьми, представив новое промежуточное звено, состоящее из сложного комплекса основанных на технологии "образований" (включая сети, цифровые услуги, базы данных, социальные сети). Поэтому, имея дело с доверием между людьми, в этой технологической инфраструктуре мы также должны учитывать аспект доверия (или уверенности).

Ниссенбаум[[50]](#footnote-50) рассматривает только доверие между людьми, которое используется в сетевых цифровых системах для общения, и перечисляет факторы, которые систематически влияют на склонность человека доверять (или не доверять):

1 История и репутация.

2 Выводы на основе личных характеристик: например, достоинствах, рассудительности, верности, желании, чтобы другие были хорошего мнения о тебе, поведении, стиле одежды.

3 Взаимоотношения: взаимность и обоюдность, семья, принадлежность одной стороне, наличие общих интересов.

4 Выполнение своих обязанностей (пилот, водитель автобуса).

5 Контекстуальные факторы (для групп и сообществ – известность; награды и наказания; нормы; гарантии доверия или безопасности, например, обязательства или потребительское право).

Некоторые из этих пунктов, в частности 1 и 3, имеют аспекты "Доверия как скрытого интереса" по определению Хардина48. В интересах доверенной стороны действовать благотворно, чтобы, например, не потерять репутацию, что может привести к прекращению общения с доверяющей стороной (например, пилот, потерявший репутацию, может лишиться работы). Также она перечисляет препятствия для доверия в онлайновой среде:

1 Отсутствующие идентификаторы (но отмечается право на анонимность)

2 Отсутствующие личные характеристики (но отмечается право на анонимность)

3 Непонятные обстоятельства (неизвестность и запутанность создает неясность, но также и освобождает).

Третий пункт может рассматриваться просто как большая сложность в онлайновой среде. Он, конечно, дает больше свободы, но в то же время для правильного проведения сделки или сеанса связи потребуется создать еще большее доверия, а следовательно  зависимости. Ниссенбаум также отмечает, что безопасность не означает доверия. Если есть безопасность, то для доверия нет необходимости. Однако доверие позволяет людям жить в совершенном, сложном и небезопасном мире, а более высокий уровень безопасности уменьшает его полноту и совершенство. Другие авторы ставят безопасность с одной стороны шкалы доверия, на другой стороне которой располагается полностью безосновательное (наивное) доверие.

Факт того, что благодаря всемирной информационной инфраструктуре доверие (к незнакомцам) возрастает с ростом объема знаний (о них), дает основание журналу Economist утверждать, что: "Желание огромного числа людей, если дать им шанс [...], жить в других странах, а не в их родной стране, делает бессмысленным освященное временем общее мнение в политике и философии, что человеку живется лучше дома"[[51]](#footnote-51). И еще: "Ошибкой философов было предполагать, что человек, поскольку он существо общественное, должен принадлежать к какому-нибудь определенному сообществу"[[52]](#footnote-52). Тем не менее, это может быть слишком быстрым обобщением поведения меньшинства, как например, все еще подавляющее меньшинство людей путешествует чаще и дальше, чем предлагается в комфортабельных надежных программах путешествий на праздники, организуемых надежными агентствами.

Тем не менее, глобализация, движимая безусловно новыми ИКТ и Сетью, создает взаимопонимание, а, следовательно, рождает большее доверие, распространяя информацию об истории и репутации обществ, характеристиках сообществ и жизни людей в определенных сообществах, позволяя с легкостью осуществить всемирное общение. Это, несомненно, может привести к дальнейшему размыванию идеи о том, что "человеку лучше всего живется дома". Также это может привести к необходимости абсолютно нового взгляда на сообщества и их единство и на ту роль, которую во всем этом должно играть доверие.

Доверие в цифровом обществе

Как говорилось ранее, следует различать:

• Доверие между людьми в обществе, которое позволяет всесторонне использовать цифровые технологии для общения и проведения сделок.

• Доверие или уверенность людей в инфраструктуре цифровых сетей и систем, которыми они пользуются для оказания услуг, общения, хранения данных, вычислений и пр.

Начнем с первого пункта.

Проблема доверия (между людьми) в цифровом обществе по сравнению со "старым обществом" в частности относится к:[[53]](#footnote-53)

• Изменению способов сбора, хранения, обработки, доступности и защиты данных. Собираются и хранятся данные, созданные не только людьми с целью их обмена и хранения, но собираются также данные о деятельности людей посредством средств наблюдения (от прогулок по улице до посещений веб-сайтов или открытия веб-страниц).

• Идентификации, репутации, аутентификации и подотчетности, которые имеют в интернете разные значения. Кому-то требуется подтвердить признаки, предоставить секретную или биометрическую информацию для подтверждения чьей-то идентичности. Репутацию легко можно разрушить, распространив вызывающую подозрение или ложную информацию, что крайне сложно исправить. Возможность скрыться под юрисдикцией других стран в значительной степени препятствует процессам подотчетности и прозрачности, если нет международных соглашений в области правоприменения и экстрадиции.

• Увеличению сложности, малопонятным технологиям с недостаточными гарантиями, даваемыми сертификацией и стандартизацией, и недостатку прозрачности процессов и методов сбора и использования данных, в результате чего возникает непонятный контекст, препятствующий доверию, необходимому между людьми в цифровом окружении. Люди могут быть сбиты с толку тем, что происходит вокруг них и зачастую не имеют понятия о том, какие данные о них собирают и как их используют.

Доверительные отношения легче установить, когда известна или может быть подтверждена (например, доверенной третьей стороной) идентичность и/или другая информация для аутентификации (мандаты, признаки или заявления) третьей стороны. Репутация и другая информация из Сети или от друзей в социальных сетях может дать больше оснований для доверия. Более того, граждане будут больше доверять сделкам с третьей стороной, если смогут управлять предоставлением и обменом своими данными с этой третьей стороной. Также доверие можно укрепить при помощи прозрачных действий сборщиков и обработчиков данных и благодаря репутации таких объектов.

Но, и это приводит нас ко второму пункту, в нашем технологическом мире такого доверия между людьми можно достичь, только если существует доверие к системам, которые используются для общения, обмена данными или подтверждения идентичности и другой информации, например, репутации или мандатов. Для того чтобы пользоваться интернетом, граждане должны быть уверены в инструментах, системах и инфраструктуре, которыми они пользуются для совершения сделок и общения. Мы называем систему или услугу *заслуживающими доверия* в определенной степени, если можно получить определенный уровень допустимого доверия к тому, что система или услуга будут оказаны в соответствии с их описанием и заверениями, и что не будет выполняться действий, которые не описаны в разных обстоятельствах. Допустимое доверие может быть оказано благодаря подотчетности (ответственности за продукт), прозрачности в обработке и хранении данных, технической сертификации системы и возможности фактического проведения аудита. Также его можно укрепить, предоставив понятные и полезные инструменты и механизмы, чтобы дать возможность подтверждать заявления на мандаты, репутацию или идентичность. Людям требуются услуги и инструменты, которые могут им помочь создать и укрепить доверие в качестве услуг, безопасности, устойчивости, защите и неприкосновенности данных, в соответствии с заранее установленными и понятными правилами. Их можно получить как через поставщиков услуг третьей стороны, так и органы государственной власти.

Как утверждает Виталий Цыгичко,[[54]](#footnote-54) особо важную роль в современном обществе играют автоматизированные информационные системы (АИС), которые становятся все более интегрированными в системы государственного управления во всех секторах национальной экономики. АИС составляют ядро систем принятия решений практически во всех социально-экономических организациях. От их работы зависит не только эффективность работы органов государственной власти, экономических и общественных организаций, но и национальная безопасность, которая в большой степени зависит от надежности работы АИС.

Несомненно, чрезвычайно важно учитывать надежность этих систем. В первую очередь это относится к действенности их основных систем, надежности их программных и аппаратных средств, уровню профессиональной квалификации персонала, обслуживающего систему и эффективности мер по ее защите от внешних угроз.

Согласно аргументам Цыгичко, надежность развития АИС требует создания комплекса требований и системы показателей для безопасности, надежности (включая основные модели в качестве отражения реальности) и целостности данных. В качестве одного из критериев оценки может использоваться измерение рисков нарушения защиты системы. **Управление рисками** определяется как процессы, включающие идентификацию риска и анализа и принятия решений, включая увеличение положительных и уменьшение отрицательных включений случаев рисковых событий.

Дополнительно к техническим средствам, необходимым для создания доверия, нам потребуются правила, регуляторные указания и общественное признание. Граждане смогут доверить обработку своих личных данных в пределах своего сообщества, если: конфиденциальность и регуляторные положения по защите личных данных выполняются и обеспечены правовыми санкциями; организации соответствуют представлению граждан о культуре подотчетности при условии соответствующей защиты потребителей и регуляторных положений о возмещении вреда; существуют регуляторные указания по ревизиям и прозрачности; и обеспечено четкое распределение ответственности по цепочке действующих субъектов сделки.

На уровне общих правил, надежная инфраструктура ИКТ может быть создана и может поддерживаться только при помощи надлежащего и честного распределения средств поощрения по всей цепочки создания стоимости.

Прозрачность и подотчетность должны гарантировать справедливость и обеспеченность правовыми положениями. Следует рассмотреть проблемы ответственности систем и, в частности, их программного обеспечения и части, отвечающей за целостность данных. Это может привести к развитию систем гарантий безопасности от рисков взлома систем, которые в свою очередь помогут созданию мер и инструментов, позволяющих проводить оценку рисков. Все это со временем может привести к созданию в значительной степени саморегулируемой и устойчивой системы.

Важным требованием для создания доверия между людьми при помощи интернета является создание всемирной надежной системы взаимодействия для **идентификации и аутентификации.** Например, вомногих странах правительство создает надежные электронные идентификационные карты и паспорта в соответствии со стандартами, которые утверждены во всем мире. Но для совершения электронных сделок в мировом масштабе требуется возможность взаимодействия управлением в интернете заявлениями и мандатами, которое будет гарантировать соответствие праву на конфиденциальность. Подотчетность важна для интернет коммерции, и ее можно обеспечить только с помощью эффективной ответственности людей и организаций за их общественные и договорные действия. Договорные действия обычно выполняются при подтверждении мандатов, демонстрации признаков или использования секретной информации, известной только данному человеку. В разных ситуациях можно использовать разную секретную информацию, мандаты или признаки, что ведет к появлению разных "идентичностей". Стандарты метауровня для управления заявлениями об идентичности были предложены Кэмероном, Пошем и Ранненбергом[[55]](#footnote-55).

Интернет с его множеством различных социальных сетей также дает людям и организациям возможность создания своих комментариев, круга друзей и репутации в разных сообществах. По терминологии проекта FIDIS[[56]](#footnote-56) это приведет к "частичным идентичностям" человека. Когда ситуация требует подотчетности, ее можно связать при помощи защиты конфиденциальности с идентификацией, аутентификацией и цифровыми подписями. Это также может помочь создать более доверительные отношения в интернете в качестве механизма для общественной и экономической деятельности.

**Резюме**

Мы рассмотрели важность и разные взгляды на доверие в нашем обществе. В частности мы рассмотрели изменения и проблемы, возникшие, когда наше общество стало все больше зависеть от цифрового общения и проведения сделок через интернет. Недостаток необходимой идентификации, учитывая необходимость анонимности в некоторых случаях, отсутствие опыта в личных характеристиках наряду с необходимостью защиты конфиденциальности и, наконец, но не менее важно, непонятный контекст, созданный технологической инфраструктурой, применяемой для нашего общения, лишили людей важных механизмов создания доверия, позволяющих им жить и творить в глобализованном обществе.

Поэтому в цифровом окружении мы должны создать новые надежные механизмы, которые дадут людям возможность создавать доверительные отношения друг с другом, вне зависимости от того где они находятся или как познакомились.

Мы должны гарантировать безопасные и надежные сети связи; информационные системы, дающие уверенность в соответствии законам о защите данных и конфиденциальности; надежную всемирную структуру, позволяющую взаимодействовать, для идентификации и управления мандатами/заявлениями; и услуги, удовлетворяющие законам об обязательной ответственности и защите прав потребителя. Такая технология должна создаваться и развиваться с учетом доверия, безопасности и конфиденциальности, и должна обеспечивать правоприменение и прозрачность, кроме того, следует разработать законы и регуляторные положения с учетом технологических тенденций и возможностей.

На международном уровне государственный и частный секторы должны работать вместе для создания хорошо сбалансированной технологической инфраструктуры и законодательства/регуляторных положений, которые дали бы гражданам уверенность в использовании своих возможностей в новом цифровом мире.

Сделав это, человечество сможет получить неожиданные вплоть до настоящего момента возможности для общения, взаимодействия и совершения экономических сделок на мировом уровне на основе механизмов доверия, похожих на те, которые мы использовали в небольших сообществах для прямого взаимодействия между людьми. Это будет решительным шагом к мировой стабильности.

## 3.2 Социально-экономические последствия киберпреступности

**Жак Бус (Jacques Bus)**[[57]](#footnote-57)

Предоставление цифровых услуг и в целом цифровая инфраструктура, созданная для нашего общества, имеют колоссальный положительный потенциал. В то же время, как и все технологии, ее можно использовать для злоумышленных деяний. Мы различаем следующие четыре проблемные области, относящиеся к социально-экономическим вопросам:

1 **Глобальная природа цифрового пространства**: Появление международных услуг и средств связи в интернете ставит множество социальных и экономических вопросов и вопросов национальной безопасности, которые до настоящего времени решались на границах государств (контроль импорта и экспорта, паспортный контроль, таможенные вопросы, межнациональные конфликты и пр.) или внутри страны при помощи действий полиции на местном или национальном уровне в отношении зарегистрированных граждан. Маловероятно, что негативные последствия нереальности пограничного контроля в цифровом пространстве рассматривались в каком-либо серьезном ключе, на уровне национального государства или на международном уровне. Однако очевидно, что это упрощает процесс совершения преступления, создавая возможность неприкосновенности для преступников, частично из-за того, что действия в Сети трудно связать с конкретными субъектами, а частично из-за того, что субъекты находятся в государствах, которые предоставляют им защиту от международного правоприменения.

2 **Сложность услуг:** Сделки и услуги в Сети все чаще приобретают вид специальных цепочек субуслуг, которые разбросаны по разным юрисдикциям и используют данные из всего мирового массива. Эти субсуслуги или данные могут подчиняться разным, порой противоречащим друг другу режимам. Потребители испытывают трудности в понимании этой ситуации и ее последствий. Государства более не могут гарантировать ответственность за продукцию и защиту своих потребителей в том же объеме, что и раньше. Для того чтобы справиться с этим, им потребуются международные соглашения и сотрудничество в области соблюдения законов. Более того, услуги должны гарантировать прозрачность цепочки услуг и (автоматически) реагировать на выставляемые потребителями условия. Существующая ситуация, наряду с пунктом первым, дает широкие возможности для не оставляющих следов мошеннических и недобросовестных действий. В настоящее время не возможно обеспечить защиту от этого.

3 **Социальные сети и тематические чаты** часто используются длязавязывания отношений с преступными целями, в частности с акцентом на детях или подростках. Это не новость. Аферы и мошеннические действия были всегда. Однако слабые механизмы аутентификации и недостаток механизмов безопасности и защиты конфиденциальности для мандатов (например, имени, данных о месте рождения, возраста, пола, данных о работе, паролей) делают это занятие очень простым и выгодным. Также в социальные сети проникли вирусы, так как это среда, в которой доверие может использоваться как вектор. Доля успешных атак при помощи социальных сетей очень велика. Фишинг является самой главной угрозой для банков, но банки пока не предлагают услуги своим клиентам собственной аутентификации.

4 **Международная организация преступлений:** Во многих публикациях сообщалось, что за последние несколько лет преступления на международном уровне не просто перешли в Сеть для воплощения своих преступных намерений, но и международный черный рынок использует интернет в качестве своего инструмента (ботнеты, инструменты для фишинга, вирусы и т. п.) и для кражи данных (личной информации, данных кредитных карт, секретной информации компаний). Преступления в Сети и с ее помощью во всем мире становятся все лучше организованными, широко распределены по юрисдикциям, включая те, где очень слабая судебная власть и серьезно ориентирована на финансовые задачи. Существует множество примеров этого развития. В марте FTC закрыла теневую компанию, выпускающую поддельные антивирусные программы, имевшую ежегодный оборот 180 миллионов долларов США. Существуют гарантии возврата денег в области вирусов, техническая поддержка и наборы "сделай сам" для совершения преступлений. На черном рынке троянская программа для взлома банковской защиты Zeus стоит 700 долларов США (4000 долларов США за последнюю версию). Zeus используется для обмана схем аутентификации, например, двухфакторных схем и схем кодов безопасности Mastercard. Есть несколько слоев легальных и теневых поставщиков, получающих выгоду от серой экономики.

Исследования и статистические данные иногда сообщают об ошеломляющих значениях потерь в социальной и экономической сфере от этих незаконных действий. Они могут достигать 1 триллиона долларов США[[58]](#footnote-58) по всему миру, что равно почти 2% всемирного ВВП. Компания Boston Computing Network оценивает потери американского бизнеса в размере более 7,6 миллиардов США в результате вирусных атак в течение первых шести месяцев 1999 года. Показатели финансовых потерь в Германии от фишинга оцениваются в 15 миллионов евро ежегодно, а от мошенничества с кредитными картами в 155 миллионов евро.

В целом большинство показателей финансовых потерь основаны на спорных предположениях и являются обязательными экстраполяциями того, что известно, хотя о многих проблемах общественности не сообщается. Тем не менее, выводы заключаются в том, что цена киберпреступности на социально-экономическом уровне весьма значительна и зачастую недооценивается теми, кто должен принимать решения о вложениях в механизмы безопасности. Дивиденды от вложений в безопасность должны рассматриваться более серьезно.

Борьба с киберпреступлениями требует необходимости назначения ответственности за действия в цифровом окружении. Это включает в себя субдеяния в динамически созданной распределенной по всему миру службе. Необходимо сотрудничество на самом высоком международном уровне в области законодательства и дипломатии, для того чтобы определить общие правила и процедуры, которые создают надежности и ответственности за услуги и общественные и экономические действия.

Для поиска решений требуется техническое развитие, чтобы с одной стороны была бы всемирная неразрывная сеть, к которой имели бы доступ компании и потребители для работы, общения и обмена информацией, дома и в дороге, при условии соответствия законам, применяемым на всех уровнях деятельности. С другой стороны люди имеют право на частную жизнь в Сети, а потому должны иметь возможность действия в Сети в рамках ограниченного надежного и безопасного круга, который они выбрали сами в определенных обстоятельствах и с гарантиями от поставщиков в том, что их обмен данными не используется для других целей.

К сожалению, в настоящее время мы наблюдаем развитие экономики конфиденциальных данных, которая движется в противоположном направлении. Компании, собирающие и обрабатывающие данные, получают доходы только при помощи бизнес-модели, относящейся к конфиденциальным данным пользователя. Потребители могут подумать, что они являются клиентами этих поставщиков услуг, и, следовательно, отвечают за свои услуги. Но на самом деле, так как потребители ничего не платят таким компаниям, фактически они сами являются продуктом. НАСТОЯЩИМИ потребителями являются маркетинговые компании, аналитики, психологи, рекламные компании, которым сайты социальных сетей, порталы услуг и т. п. продают данные о пользователях.

На самом деле, кажется, что личная жизнь стала жертвой социально-экономической среды, связанной с цифровизацией и сетями. Ценой за хранение данных стало очень быстрое и безостановочное уменьшение объема данных, который можно хранить без ограничения качества и времени. Это будет иметь большое влияние на способы нашего взаимодействия, а также породит в будущем как новые преступления (нарушения конфиденциальности, незаконное профилирование, незаконный сбор данных), так и новые способы политического управления. Многое из этого может противоречить существующим конституционным правам, и ведутся серьезные обсуждения того, как это отразится на социальной, экономической и политической стабильности в обществе.

Дополнительно к обсуждавшимся ранее возможным воздействиям цифрового окружения на преступность и права человека, совершенно отличная опасность для общества и экономики связана с крайней уязвимостью будущих цифровых социальных инфраструктур. Общество в целом может столкнуться с серьезными экономическими и социальными потерями, когда их сети связи или другие важнейшие инфраструктуры будут атакованы и разрушены преступниками (с целью вымогательства), террористами с целью распространения страха и нестабильности, или другими государствами в ходе военных действий или в целях устрашения. Возможность государства противодействовать таким атакам практически сводится к защитным действиям. Более агрессивные стратегии, например, устрашение или контратаку, трудно реализовать, так как такие атаки зачастую не имеют отличительных признаков и часто проводятся из неизвестных мест или экстремистских государств. Если не уделить достаточно внимания безопасности и надежности сетей и систем, технологическое развитие усугубит эти проблемы и может привести к национальным и международным конфликтам, которые могут стать неконтролируемыми в будущем.

Наконец, важным и дополнительным элементом, на который следует обратить внимание, являются более долгосрочные риски для общества. Атаки могут длиться несколько секунд, и иметь при этом намного более длительные последствия. Для того чтобы восстановить доверие общества, потерянное за эти секунды, могут потребоваться годы. Подрыв доверия между людьми, между клиентом и бизнесом, между гражданами и государством, а также между государствами в течение долгого времени может оказывать разрушительное воздействие на общественную стабильность на мировом уровне. В будущем могут возникнуть препятствия для эффективного экономического роста, который в современной посткризисной экономике в значительной степени зависит от роста объемов использования ИКТ. Мы не можем позволить себе застой в этой области из-за потери доверия.

Безопасность сети и информации, включая аутентификацию, в цифровом окружении должны гарантировать безопасность граждан (физическую, экономическую и личную). Надежные системы, инфраструктуры и организации ИКТ гарантируют в наших обществах определенный уровень социального доверия, что, как показали многие исследования, важно для экономического процветания.

Сложно измерить уровень социальной нестабильности и экономического ущерба (в показателях экономического роста), но он может быть очень высок. Он является стимулом для создания как механизмов готовности и крепкой защиты, так и систем быстрого восстановления и самоисцеления.

**В заключение мы можем сказать:**

Глобальный характер цифрового пространства со слабыми механизмами идентификации пользователей и недостаточной определенностью источников действий, комплекс распределенных по всему миру услуг, всемирное развитие социальных сетей, а также появляющиеся сети и рынки международной преступности обуславливают серьезную обеспокоенность ростом киберпреступности, и ее влиянием на устойчивое развитие стабильного общества как основы личного развития и экономического процветания.

Уязвимость наших инфраструктур ИКТ и отсутствие ограничений для сбора данных угрожают личной свободе и международной стабильности.

Доверие, которое граждане испытывают к обществу и правительству, надеясь, что они защитят их мирное существование, безопасность и благополучие, подрывается угрозами и неопределенностью, обусловленными техническим развитием с возможными большими экономическими потерями.

Поэтому нам крайне необходимы глобальные политические действия, направленные на решение этих проблем, основанные на убедительном анализе тенденций и последствий в технологической, социальной, экономической и политической областях.

# 4 Тенденции и угрозы в технологической сфере

## 4.1 Существующие возможности, тенденции и угрозы

**Аксель Лехман (Axel Lehmann), Владимир Бритков (Vladimir Britkov), Жак Бус (Jacques Bus)**

Движущей силой для обновления продукции является как технологическое "давление", так и рыночная "привлекательность". С этой точки зрения в ходе анализа будущих направлений и возможностей инноваций в ИКТ следует учитывать как существующие и ожидаемые технологические прорывы, так и тенденции потребления в будущем или потребности рынка. Поэтому первые три раздела данной главы посвящены этим тенденциям и потребностям с соответствующим последующим анализом основных угроз и некоторыми завершающими замечаниями.

Для того чтобы начать эту главу с краткого изложения результатов последующих анализов и оценок, мы предполагаем, что ожидаемые технологические инновации обусловят не только быстрое развитие новых микро- и нанотехнологий, но и развитие крупносерийного производства встроенных датчиков и счетных устройств, новых сетевых технологий и технологий связи, инновационных услуг и приложений. Эти инновации также дадут возможность движения в двух главных направлениях развития:

• конвергенция существующих отдельных компьютеров и мобильных телефонов в единые портативные многоцелевые устройства для вычислений и связи; и

• развитие существующего интернета, веб-технологий и услуг в направлении интернета будущего. "Интернет вещей", для которого будет характерен большой объем связи и подвижности, как для людей, так и для различных устройств и объектов ("вещей") станет шагом вперед к эффективному, надежному и заслуживающему доверия интернету будущего.

Такой технологический прогресс будет подкреплен потребностями рынка и потребителей в создании продуктов, услуг и приложений ИКТ. Согласно опубликованному журналом Forbes исследованию, отрасли развлечений и связи, энергетики и здравоохранения будут во главе движущих сил и основными областями применения инновационных продуктов ИКТ[[59]](#footnote-59).

С этой точки зрения, в следующих подглавах будут описаны основные силы воздействия на развитие ИКТ в будущем и его последствия: технологические тенденции, потребности рынка и потребителя и "интернет вещей", а основные шансы, угрозы и проблемы, связанные с воздействием этих инноваций в ИКТ на нашу частную и общественную жизнь, обобщены в последних двух подглавах.

Технологические тенденции

Нет никакого сомнения в том, что в текущем десятилетии миниатюризация и цифровизация внесли весомый вклад в большой рывок вперед по направлению к "цифровому миру", в котором все данные, информация и знания хранятся, передаются и обрабатываются в цифровой форме. Анализ тенденций будущего развития существующих основных технологий и полупроводников, показывает, что закон Мура, гласящий, что "количество транзисторов на квадратный дюйм удваивается каждые два года", вероятно будет действовать, как минимум, еще лет десять. Существующие технологии разработки и производства позволяют встраивать в один чип несколько миллиардов транзисторов. Даже если в долгосрочной перспективе существующие полупроводниковые технологии будут постепенно заменяться новыми технологиями, например, биотехнологиями или квантовыми вычислениями, эти общие тенденции увеличения объемов миниатюризации и цифровизации, расширенных функциональных возможностей и применимости будут существовать и обеспечивать дальнейшее расширение продуктов и приложений ИКТ или на основе ИКТ.

С этой точки зрения в контексте улучшения аппаратного, микропрограммного и программного обеспечения следует рассмотреть четыре основные области развития цифровых систем и принципов организации:

• Отдельные и множественные компьютерные системы.

• Сети, протоколы и услуги связи.

• Нанотехнологии, материаловедение, датчики, действующие субъекты и встроенные системы.

• Децентрализованные механизмы работы и организации для цифровых систем.

Поскольку очень большое скопление транзисторов на площади чипа и увеличение тактовой частоты создает проблемы перегрева, существующие **микропроцессоры** строятся в виде многоядерных процессоров, работающих со сниженной тактовой частотой, а увеличение рабочих характеристик достигается за счет выполнения параллельных процессов на одном чипе. Дальнейшие работы в области улучшения процессоров будут возможны благодаря многоуровневым полупроводниковым технологиям, которые увеличат количество ядер в процессоре и снизят энергопотребление в чипе. Это приведет к серьезным улучшениям рабочих характеристик, благодаря многоядерным процессорам, многопроцессорным системам, дальнейшему увеличению возможностей сверхоперативной и оперативной памяти, и развитию системы-на-чипе. Эти тенденции улучшат рабочие характеристики всего спектра компьютеров, от однокристального компьютера и встроенных вычислительных компонентов до суперкомпьютеров. Так как сети связи и коммутации также будут развиваться, будут доступны все виды структуры и архитектуры взаимосвязанных компьютеров.

Дополнительно, благодаря улучшенным технологиям миниатюризации будут доступны устройства быстрого внешнего хранения с расширенными возможностями хранения и сокращенным временем доступа. Наряду с улучшенными архитектурными подходами и программными технологиями будет осуществимо крупномасштабное параллельное выполнение комплексных программных приложений. Параллельно, благодаря развитию новых энергосберегающих технологий и аккумуляторов, будет существенно расширена или упрощена подвижность компьютеров и всевозможных вычислительных устройств.

В области **сетей, протоколов и услуг электросвязи,** основные инновации являются результатом постоянных улучшений техники беспроводной и спутниковой связи, предлагающей более высокую степень соединенности и рост пропускной способности. Одна из основных тенденций касается динамического формирования виртуальных сетей, например, виртуальных частных сетей[[60]](#footnote-60). Этот метод, который уже применяется, предлагает ограниченное во времени формирование и использование приложений и ориентированных на пользователя сетей, состоящих из выбранных компонентов сетей и услуг.

Другая тенденция повышения гибкости и удобства использования существующих вычислительных и коммуникационных инфраструктур связана с формированием наложенных сетей. В настоящее время этот технический подход, являясь основной темой исследований, рассматривается как эффективный способ преодоления известных ограничений существующих протоколов IP/TCP и развития от IPv4 к IPv6, что представляет собой важные шаги к расширенному использованию интернета, и "Интернета вещей". Оба направления технического прогресса являют собой предпосылки для дальнейших инноваций технологии интернета и технологии приложений. Беспрецедентный рост современного интернета, особенно в том что касается разнообразия и количества подключенных к интернету объектов, требует, с одной стороны значительного расширения существующего адресного пространства интернет-объектов (IPv4) до IPv6[[61]](#footnote-61). Следовательно, должны быть разработаны специальные методы преобразования, позволяющие выполнять масштабируемый переход между этими двумя стандартами. С другой стороны, и одновременно с эволюцией от IPv4 к IPv6, должно быть обеспечено развитие будущих стандартизированных IP/TCP протоколов, которые обеспечили бы связь между всеми видами объектов посредством "интернета будущего". Несмотря на то, что оба направления исследований по-прежнему требуют конкретных решений, можно предположить, что эти технические основы для будущего интернета будут использоваться в течение нескольких лет, предоставляя лучшие и новые возможности для интернет приложений, например, для "Интернета вещей".

В дополнение к вышеупомянутым тенденциям развития ИКТ системы, в ходе анализа будущих тенденций и угроз со стороны ИКТ необходимо учитывать быстрый технический и производственный прогресс в нанотехнологиях, материаловедении и в специальных цифровых компонентах, таких как полупроводниковые датчики, операторы или встроенные системы. Эти достижения приведут к созданию таких ИКТ-компонентов, как:

• Практические интерфейсы пользователя[[62]](#footnote-62).

• Полимерные дисплеи.

• Цифровые одежды (миниатюрный компьютер)[[63]](#footnote-63).

• Пассивные и активные датчики (технологии RFID [[64]](#footnote-64)).

• "Окружающие умные[[65]](#footnote-65)" или "интеллектуальные "системы.

Наряду с этими техническими достижениями, улучшенные и новые **продукты прошивки/программ**, **услуги** и организационные механизмы откроют возможности для улучшенных и дополнительных функций и услуг. Эти достижения лежат в диапазоне от различных инновационных технологий, программного обеспечения, например, разработки программного обеспечения на базе агентов, сервисно-ориентированной архитектуры (SOA), новых веб-услуг или систем управления, например, для эффективного хранения и извлечения данных, для эффективной балансировки нагрузки, до эффективного использования GRID-инфраструктуры, образованной из огромных сетей распределенных компьютеров и ресурсов электросвязи. Наиболее актуальными и многообещающими приложениями являются сетевые вычисления или облачные вычисления[[66]](#footnote-66), которые открывают новую эру инфокоммуникационных технологий в том, что касается их экономики, производительности, доступности и надежности.

Кроме всех описанных выше технологических достижений, при анализе важнейших тенденций и угроз для инноваций в области ИКТ особенно следует учитывать две основные, фундаментальные тенденции, касающиеся **организации и принципов работы:** **виртуализация и децентрализации**. Постоянное расширение функциональных возможностей и возможностей взаимосвязи с разнородными электронными компонентами, с одной стороны, и рост потребности в их эффективном использовании, с другой стороны, привели к созданию и эксплуатации виртуальных систем, таких как виртуальные процессоры, виртуальные хранилища или даже виртуальные компьютеры. Кроме того, постоянно растущая сложность связанных в сеть компьютеров и систем электросвязи, а также использование виртуальных сетей, как отмечалось выше, часто мешают эффективной работе в условиях централизованного управления. Вместо этого, применяется все больше и больше операционных механизмов для децентрализованной системы управления, которая оказалась более гибкой и эффективной, чем централизованная. Примерами последней являются агентские программные приложения или биоаналоговое управление системой.

Реализация и совместное применение обоих принципов  виртуализации и децентрализации  уже привели к созданию новых возможностей эффективного использования цифровых ресурсов, соединенных в сеть. Такие сети могут образовывать "сетки"[[67]](#footnote-67): компьютерная сетка, состоящая из соединенных в сеть узловых компьютеров, сетка данных, создаваемая из взаимосвязанных систем распределенного хранения данных, или сетка оборудования, созданная из специализированных устройств, к которым может быть организован удаленный доступ. В случае облачных вычислений доступ к этим сетевым и взаимосвязанным ресурсам может быть удаленным, а использовать их можно через поставщиков. Помимо этих экономических преимущества и выигрыша в производительности, следует рассмотреть и риски тоже. Основная проблема  и в настоящее время основной риск – касается того, как справиться со сложностями этих систем, особенно в отношении безопасности, надежности и защищенности. Учитывая современное состояние науки, те сетевые системы, которые уже находятся в эксплуатации  не могут быть ни полностью проверены на правильность работы, ни полностью проверены для конкретных приложений, и не испытаны полностью из-за их огромного пространства состояний. Эта ситуация до сих пор не получила должного внимания, хотя она раскрывает фундаментальную проблему инноваций в

области ИКТ[[68]](#footnote-68). Кроме этой проблемы существуют и дополнительные риски, обусловленные появлением ошибок и сбоев, а также другими источниками потенциальных злоупотреблений и манипуляций. Эти риски должны учитывать общую оценку этих инноваций ИКТ и крайне необходимо выполнить еще множество исследований возможных контрмер.

Тенденции требовании рынка и потребителей

Уже сейчас основные требования рынка и потребителей касаются технологий повсеместных вычислений, связи и доступа к информации, что означает использование цифровых устройств и сетевых возможностей "в любом месте в любое время". Высокая мобильность потребителей, с одной стороны, и глобальное распространение и доступность информации и знаний, с другой стороны, повышают спрос на улучшенные или дополненные функциональные возможности ИКТ продуктов и их эффективное использование. Эти требования будут постоянно и значительно расти и формироваться различными рынками. Например, существует растущий спрос на локально распределенное и не зависящее от времени сотрудничество в разных отраслях промышленности и странах

Все эти требования неявно основаны на предположении, что мы собираемся жить и работать в полностью цифровом мире, где каждый отдельный объект или каждый элемент информации можно получить и использовать в любое время и в любом месте. Эти требования рынка и потребителей образуют значительный "набор" для технологических инноваций, например, эффективное использование мультимедийных и видео приложений, повсеместный доступ к всемирной паутине, коллективная работа с использованием компьютеров (CSCW) или использование огромного разнообразия интернет-услуг и приложений. Помимо новых и полезных ИКТ компонентов и продуктов, движение в сторону создания "Интернета вещей" может создать новые социальные и управленческие проблемы, а также потенциальные угрозы для безопасности и защищенности. Следовательно, эти инновации и их последствия необходимо тщательно проанализировать с самого начала – что означает непосредственно сейчас (см. следующий подпункт).

Как описано выше, текущие и будущие достижения в области оборудования/прошивок/программного обеспечения позволят создавать новые ИКТ‑продукты и инновационные приложения в этих направлениях и для различных областей применения. Примерами таких областей применения являются:

• Проживание с уходом со стороны окружающих (например, для пожилых людей)[[69]](#footnote-69).

• Интеллектуальные системы управления (например, в сфере транспорта, логистики, воздушной навигации, энергосбережения, и т. д.).

• "Умные" дома[[70]](#footnote-70).

• Здравоохранение.

Хотя требования в секторах развлечений и общения сосредоточены, главным образом, на ИКТ, аспектах качества и экономики, другие прикладные области, например, системы управления или наблюдения в секторах энергетики и здравоохранения должны, прежде всего, соответствовать требованиям по безопасности, надежности или защищенности. Как упоминалось в предыдущем подразделе, постоянно растущее число и расширяющиеся возможности цифровых устройств, используемых в этих приложениях, вместе с их практически неограниченными возможностями для взаимосвязи приводит к возникновению проблемы "взрыва пространства состояний". В срочном порядке необходимы активные усилия в области фундаментальных и прикладных исследований, для того чтобы разработать адекватные дизайн, методы верификации и валидации, а также стратегии тестирования для выполнения этих требований к качеству.

**"Интернет вещей"**

"Интернет вещей" это концепция, согласно которой в будущем к интернету помимо людей могут быть подключены все виды объектов, устройств или товаров из нашей повседневной жизни ("вещи"). Эти "вещи" смогут принимать, хранить, обрабатывать или передавать данные и информацию в ходе общения с другими "вещами", людьми или услугами. Для этого требуется, чтобы как можно большее число "вещей" имело бы интернет-адрес, что станет возможным в IPv6  и работать самостоятельно или в составе

подсетей, как физический источник, место назначения или точка доступа для общения, взаимодействия и вычислений[[71]](#footnote-71).

Поэтапное осуществление этой концепции может реализовать идею "повсеместные вычисления и связь", которую около 20 лет назад высказал Марк Уэйзер (Mark Weiser) [[72]](#footnote-72). Основной характеристикой этой концепции является разработка технических объектов, приближающихся к "интеллектуальным объектам", которые имеют ограниченные возможности вычисления и рассуждения, и которые связаны с киберпространством через интернет. Примером такого "интеллектуального объекта" может быть активный датчик, который получает информацию от других объектов, обрабатывает эту информацию и, зная ее текущий статус, реагирует, посылая ответные сообщения другим объектам. Это позволит осуществить общение не только между людьми и "вещами", но также и между самими "вещами", давая приложениям совершенно новые возможности, и подвергая их риску в том, что касается защищенности и ИТ-безопасности (конфиденциальности, подлинности, защиты данных).

Современные угрозы

Как упоминалось ранее, масштаб, сложность и открытость нашего мира, соединенного в цифровые сети достигли того уровня, на котором не удивительно, что злоупотребления растут быстро, и тенденции будущего расширения ИКТ еще больше увеличивают количество и вероятность угроз, если не к ним не относиться с должным вниманием.

Получено множество сообщений, либо заинтересован в продаже ИКТ решений в области безопасности, например, MacAfee[[73]](#footnote-73), Symantec[[74]](#footnote-74), Kaspersky[[75]](#footnote-75), или от тех, кто обсуждает более общие вопросы безопасности или заинтересованы в безопасности своих IT-систем и продуктов[[76]](#footnote-76). В этих докладах в основном рассматриваются следующие категории методов киберпреступности:

1 **Вредоносный код или вредоносные программы**, программное обеспечение, основанное на ощутимом намерении его создателя, а не на каких-либо конкретных функциях. К вредоносным программам относятся компьютерные вирусы, черви, троянские кони, шпионские программы, нечестная реклама, преступные программы, большинство руткитов и другое вредоносное и нежелательное программное обеспечение[[77]](#footnote-77). Компания Symantec сообщила о том, что с 2007 года по 2008 год число новых вредоносных программ выросло с 624 000 до 1 656 000.

2 **Спам** – это злонамеренное использование электронной системы обмена сообщениями, включая большинство вещательных СМИ и цифровые системы доставки, для рассылки все подряд огромного количества нежелательных сообщений. Наиболее часто используемым видом спама является спам в электронной почте или передача нежелательных сообщений электронной почты коммерческого содержания, которые рассылаются в больших количествах. При небольшой стоимости отправки потенциально создаются высокие доходы. Однако все чаще, спамовые сообщения рассылается с преступными намерениями, и содержат вредоносные программы или с намерением ввести людей в заблуждение, побуждая их осуществить платежи, информационные релизы и т. д. (фишинг)

Для того чтобы скрыть адрес отправителя и обеспечить большие объемы рассылки, преступники часто используют "зомбированные" компьютеры или компьютеры боты (чужие компьютеры, которые работают в качестве удаленного подчиненного устройства под внешним управлением без ведома владельца) или сети "зомбированных" компьютеров, которые называют также ботнетами. По оценкам, в 2008 году в общей сложности было отправлено 350 миллиардов спамовых сообщений, и 90% из них  через ботнеты. Что составляет примерно 85% от общего числа сообщений по всему миру.

3 **Фишинг-сайты** и хосты маскируются или подменяют адрес веб-сайта или электронной почты известной организации, например, банков, с преступным намерением завладеть конфиденциальной информацией, такой как логины, пароли и данные кредитных карт. На компьютере могут быть установлены вредоносные программы, которые вместо желаемого надежного сайта отправляют пользователя на фишинговый веб-сайт, либо спам, отправленный с поддельного адреса, может предлагать пользователю перейти по ссылке на фишинг-сайт. Согласно отчетам в 2008 году обнаружено около 55 000 фишинговых хостов, что на 66% больше, чем в 2007 году.

4 **Боты и ботнеты** создаются из компьютеров многих пользователей без их ведома. Они либо непосредственно используется или "арендуются" для преступного использования на черном рынке. Компания Symantec ежедневно обнаруживает около 75 000 бот-инфицированных компьютеров, и 15 197 различных новых серверов по управлению и командованию ботами. Серверы теневой экономики поставляют на черный рынок украденную информацию (по кредитным картам, ID и т. д.) или осуществляют продажу/ аренду вредоносных программ или ботнетов.

Хотя, как правило, сообщается, что большинство атак осуществляется в США, Бразилия и Китае, нападения могут быть совершены кем угодно в любое время и даже из отдаленных мест. Хотя в нашей памяти еще свежа атака Conficker, основанная на уязвимости нулевого дня, можно сделать осторожный вывод о том, что число серьезных уязвимостей нулевого дня уменьшается благодаря повышенному вниманию к безопасности операционных систем и приложений со стороны крупных компаний разработчиков программ.

Преступные намерения фокусируются в финансовом секторе, который привлекает более 70% фишинга, на втором месте поставщики доступа в интернет, на долю которых приходится 11%.

*Белая книга*: *Новые Угрозы для ИКТ*, написанная консорциумом FORWARD[[78]](#footnote-78). Делает попытку систематического исследования новых и будущих угроз. Они определили четыре оси, на которых ожидаются в настоящее время разворачиваться будущие изменения или на которых: *новые технологии, новые приложения и новые бизнес-модели*, и *новая* *социальная динамика*. Они определили 28 угроз, поделенных на восемь категорий:

1 *Сети*: угрозы, связанные с внедрением и развертыванием новых сетевых технологий, а также услуг инфраструктуры (маршрутизация, DNS) в интернете.

2 *Оборудование и виртуализация*: угрозы из-за разработки нового аппаратного и программного обеспечения, связанные с виртуализацией и облачными вычислениями.

3 *Слабые устройства*: угрозы, появившиеся вместе с новыми вычислительными устройствами, которые ограничены, как вычислительно, так и по мощности.

4 *Сложность*: угрозы, которые возникают из-за сложности и масштабов будущих систем, которые приводят к неожиданным и непреднамеренным зависимым взаимодействиям и последствиям для безопасности.

5 *Манипулирование данными*: угрозы, которые связаны, с тем что люди (и системы) хранят все больше данных в он-лайне, и эти данные становится все более ценными и уязвимыми.

6 *Инфраструктурные атаки*: угрозы, связанные с тем фактом, что противники активно разрабатывают и развертывают наступательные платформы (например, ботнеты). Они более не выполняют атак типа "Ударил и беги", а создают в интернете оперативные базы для выполнения вредоносных кампаний.

7 *Человеческие факторы*: угрозы из-за внутренних атак, особенно в ситуации аутсорсинга, а также угрозы, связанные с новыми атаками социального происхождения.

8 *Недостаточные требования безопасности*: угрозы, связанные с традиционной торговлей коммерчески доступными товарами, методы которой строились без достаточной защиты, и в настоящее время используются и развернуты в сценариях, для которых их механизмы защиты недостаточны.

Такая классификация позволила сделать приоритетными дополнительные исследования, которые необходимы для смягчения угроз, учитывая их серьезность, ожидаемые вероятности и предпринимаемые усилия. Они пришли к выводу, что наивысший приоритет имеют угрозы, связанные с: *параллелизмом, масштабом, структурами обеспечения теневой экономики, вредоносными программами для мобильных устройств и социальными сетями*.

Современное состояние угроз является явной причиной для тревоги и требует на глобальном уровне срочных скоординированных действий экспертов в различных областях, а также политиков и дипломатов. Хотя некоторые из этих угроз требуют, в первую очередь, усилий для разработки или совершенствования правил, стандартов, методов и инструментов безопасности, для других срочно требуются основные научно-исследовательские действия и решения для практической реализации.

**Заключение**

Будущие научные исследования и разработки в области ИКТ будут оказывать существенное влияние на личностные, социальные и культурные ситуации во всем мире, как в частной, так и в общественной жизни. Современное революцион-ное/эволюционное развитие цифровых систем, интернета, а также их услуг и приложений становится основным ресурсом для повседневной жизни. Этот цифровой мир дает множество преимуществ и возможностей и для человечества, и для технического развития, а также новые способы решения некоторых глобальных проблем, таких как энергетические или проблемы здравоохранения. В этой главе рассмотрены основные возможности и преимущества будущих технологий и приложений ИКТ.

Несмотря на эти позитивные аспекты, рассматриваются более новые и более серьезные проблемы, которые требуют более интенсивных фундаментальных исследований и путей решения: основной проблемой является отсутствие методов разработки и анализа, которые согласно научным доказательствам, способны справиться с будущими взаимосвязанными цифровыми системами огромной сложности, особенно в том, что касается безопасности, надежности, функциональности и безопасности (конфиденциальность, подлинность, безопасность данных). Разработка решений для этой фундаментальной проблемы является одной из наиболее важных проблем для компьютерной науки и сообщества научных исследований в области веб-технологий. Глобальное распределение открытого "списка сложных задач", типа того, что был подготовлен Всемирной федерации ученых, вместе с эффективными контрмерами – при их наличии  может оказаться очень полезным шагом в этом направлении.

Но этот "разрыв в освоении" относится не только к современным методам разработки и производства. Всегда следует учитывать последствия ошибки человека, технические неполадки, неисправности или злоупотребления и манипуляции, и должны быть разработаны и применены контрмеры  последнее, насколько это возможно в отношении данного ограничения.

Кроме того, не хватает соответствующих мер, которые заставили бы пользователей, потребителей и организации узнать об основных проблемах, рисках, или даже угрозах, возникающих в результате использования ИКТ ресурсов. В разработке информационных материалов по ИТ-безопасности для различных аудиторий должны принимать участие профессионалы средств массовой информации. Как отмечалось в главе II, современные общества зависят от ИКТ и развивающегося интернета. Следовательно, в целях укрепления доверия следует тщательно проанализировать и обсудить последствия будущих технологических разработок в направлении создания цифрового мира.

## 4.2 Правительственная цензура интернета: Киберрепрессии

**Хеннинг Вегенер (Henning Wegener)**

Свобода убеждений и свободный доступ к информации являются центром функционирования информационного общества и необходимыми элементами киберстабильности и кибермир, определенных в главе VI в "Концепции Кибермира" того же автора. Угрозы для их осуществления снижают или опровергают основные преимущества интернета, и, следовательно, их следует перечислить в ряду основных современных угроз в киберпространстве[[79]](#footnote-79).

Свобода убеждений и свободный доступ к информации на протяжении всей истории являются ключевыми элементами в построении цивилизованного общества. Они являются неотъемлемой частью прав человека и гражданских свобод и, следовательно, лежат в основе почти всех современных конституций. Действительно, свобода личности получать информацию, иметь и высказывать мнение может служить критерием прогресса человечества. С другой стороны, определение ограничений, которые должны ограничивать эту главную свободу из соображений общественной безопасности, порядочности и *общественного порядка* всегда были неотъемлемым элементом внутренних политических дебатов, постоянными и необходимыми усилиями в стремлении к согласованию и оптимизации, как свободы личности, так и общественных интересов

Правительственная цензура, которая систематически превышает эти пределы, тщательно контролируя общественное мнение и обмен мнениями, в основном в отношении печатных материалов, является болезненной, но повторяющейся частью истории человечества, и они снова и снова развязывают битвы за свободу ума.

В эру интернета, это основное положения не меняется, но меняется его актуальность и его форма. Цифровые технологии стремительно перенесли возможности доступа к информации и связи в новое измерение; и сущность информационного общества состоит в том, что оно зависит теперь от нас. Как и в любом другом аспекте, интернет увеличивает амплитуды, смешивает количество и качество, сводит на нет расстояния и время, и создает амбивалентно новые явления.

Так как интернет не только экспоненциально увеличивает объемы информации и ее доступность, но и повышает возможности вторжения в базовые технологические процессы и управления цифровым контентом. Цифровая технология позволяет создавать фильтрующее программное обеспечение, которое может блокировать любую область информации либо во всем интернете, либо относящуюся только к определенным серверам, и это позволяет правительствам вводить правительственную цензуру, в том числе и в массовых масштабах. Следовательно, вопрос о свободе убеждений и информации, как права человека, должен рассматриваться заново: интернет быстро становится новым полем битвы в борьбе за права человека и свободу убеждений.

Основными методами, доступными для правительственной цензуры, являются IP‑блокировка, DNS фильтрация и перенаправление, фильтрации URL посредством сканирования по целевым ключевым словам или фильтрации пакетов, которое прекращает передачу TCP пакетов при обнаружении запрещенных ключевых слов. Одной из характерных черт является то, что современное фильтрующее программное обеспечение реагирует только механически на появление определенных слов или фраз, и таким образом порой "слишком часто стреляет по мишени" ("переблокировка").

Список промышленных поставщиков фильтрующего программного обеспечения, применяющих эти и другие методы  огромен. Он содержит и наиболее известные в информационных технологиях имена, и специализированные компании. Есть несколько веб-страниц посвященных сравнительной оценке и рейтингам того, что предлагают такие программы, а также их эффективности; в то время как другие страницы, управляемые сторонниками полной свободы самовыражения в интернете, критикуют само существование этой технологии

Технологию фильтрации следует рассматриваться вместе с вариантами ее обхода. Те же сложности, которые привели к разработке фильтров, характерны и для технологий, разработанных, для того чтобы их избежать, обойти или повредить. Тотальную цензуру информации в интернете осуществить очень трудно или даже невозможно, благодаря базовой распределенной технологии Сети. Таким образом, имеется множество ресурсов и решений, которые позволяют пользователям обходить цензуру в интернете. Большая их часть опираются на получение доступа к каналу интернета, который не подлежит фильтрации, часто в различных странах действуют разные законы цензуры. Очевидным вызовом для Правительства, практикующего цензуру интернета, является то, что до тех пор, пока в мире есть *одна* общедоступная система без цензуры, будет оставаться возможность доступа материалам, подвергшимся цензуре. Методы, доступные для такого скрытого доступа, включают в себя использование проксисерверов, создание виртуальных частных сетей, а также загрузку программного обеспечения с открытым кодом, которое позволяет анонимный серфинг, общение в чате и передачу файлов (примерами являются программы Psiphon, I2P, Tor).

Фильтрация контента, конечно, также играет важную функцию социальной защиты. Блокировка страниц детской порнографии, призывов к насилию, расовой ненависти и преступности в целом представляется законной для всех, это же справедливо и для более широкого использования интернета в целях внутреннего и международного терроризма. Содержание, которое не может быть законным образом распространено *за пределами* интернета, *в пределах* сети также должно подчиняться правовым санкциям и запретам. В этой связи, индустрия фильтрующего программного обеспечения удовлетворяет законные потребности.

Но здесь должно быть сделано важно различие.

Вне зависимости от эффективности фильтров, и, следовательно, действенности цензуры, и вне зависимости от связанных с ней коммерческих интересов, решающим является тот факт, что в "свободных" обществах, так называемых западных демократий с их высокой ценностью консенсуса, главным образом  но отнюдь не исключительно  ограничения на свободу убеждений и доступа к информации четко регулируется законом, сфера их применения определяется по правилу адекватности и соразмерности, и они могут быть оценены в соответствии с общедоступными юридическими процедурами. Наличие четких правовых рамок и доступность независимого юридического регулирования являются, по сути, решающими критериями для разграничения законного контроля контента и незаконной цензуры; они также предоставляют инструментарий для учета различий в культурных ценностях и определениях конфиденциальности. Контент, противоречащий культуре, религии, морали и другим глубинным целям общества в определенных странах, не должен быть освобожден от контроля под лозунгом абсолютной свободы интернета, и те, кто справедливо осуждает политическую цензуру со стороны правительства, должны проявлять осторожность и не становиться ни на какую сторону в таких вопросах,

Поскольку все вопросы, касающиеся фильтрации интернета со стороны правительства, пределов ограничений свободы убеждений, которые должны соблюдаться, противовесов, которые должны быть исключены, и роли ИТ-индустрии в предоставлении технической основы для регулирования интернета, являются сугубо деликатными вопросами национального суверенитета, настоящая статья не ставит своей целью обвинения или возложения ответственности на какое-либо отдельное правительство; действительно, здесь не названа ни одна конкретная страна. Равным образом, не указывается никакое ИТ‑оборудование, программное обеспечение или услуга. На самом деле, целью этой статьи является описание проблем и оценка состояние дискуссии, а не поспешные заключения. В том же духе сдержанности цитаты веб-страниц или статей приводятся только для информации, и они не означают, что данная статья идентифицирует себя с их содержанием или одобряет его.

Учитывая природу интернета, уменьшающую значимость границ, для регулирования свободы интернета национальные правила оказываются недостаточными. Поэтому в 1999 году Европейский союз ввел в действие новый режим общеевропейского регулирования и соответствующие процедуры допустимого вмешательства в контент интернета ("Программа Безопасный интернет"). Он опирается в основном на принцип саморегулирования интернета и поисковых машин, с тем чтобы исключить незаконный или вредоносный контент и обеспечить его соответствие национальному законодательству. В некоторых областях такие функции саморегулирования действуют удовлетворительно, хотя иногда могут потребоваться дополнительные законодательные акты.

Говоря в мировом масштабе, международные правовые нормы установлены, в частности, двумя большими договорами по правам человека в первые годы существования Организации Объединенных Наций  *Всеобщей декларацией прав человека* (1948 года) и *Международным пактом о гражданских и политических правах* 1966 года. Практически все страны подписали и ратифицировали эти пакты, которые считаются сегодня частью обычного международного правом, и, следовательно, обязательными и для государств, их не подписавших. Так совпало, что в обоих документах имеется Статья 19, где признается принцип свободы самовыражения и убеждений, и которая включает в себя право любого человека получать и распространять информацию любого типа, независимо от государственных границ и при помощи любой среды для ее распространения. Не существует никаких сомнений в том, что это право также включает в себя и получение информации через интернет, и право доступа к нему (так же, как право *не* позволять доступ), и поэтому Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО, 2003 года и 2005 года) торжественно подтвердила эти принципы в качестве центральных и неотъемлемых элементов информационного общества, в частности, в Женевской *Декларации принципов* (принципы 4, 5 и 55). Стоит отметить, что текст документов ВВУИО подчеркивает аспект свободы, уменьшая значимость предостережений, добавленных в Международный Пакт.

То, что в "свободных" обществах сводится к реально трудной проблеме определения критериев постоянного политического баланса между свободой и вмешательством государства в четких правовых рамках, во многих других государствах становится проблемой прав человека и качества глобального информационного порядка. Правительственная цензура интернета посредством технологий фильтрации без законодательных ограничений, и с серьезными и острыми последствиям для людей, собирающих и передающих информацию, является значительным нарушением прав человека. Проблематичной составляющей этого развития является то, что западные технологические компании не только предоставляют свои технологии фильтрации для правительственной цензуры, но и оказывают содействие в их использовании, создавая эффективные и действенные системы цензуры. Эта ситуация является центральной для настоящего анализа, который также имеет своей целью предложить возможности для международного противодействия такой практике. Как заметил Джо Гланвилл (Jo Glanville) редактор документа "Index on Censorship"[[80]](#footnote-80): "В настоящее время впервые в своей истории цензура является коммерческим предприятием" [[81]](#footnote-81).

Это написано в то время, когда можно видеть критический процесс роста как числа правительств, использующих цензуру интернета, главным образом в ущерб политическим правам и свободам, так и эффективности методов фильтрации.

Состояние и развитие правительственной цензуры интернета наблюдается многими частными организациями, в том числе ищущей новые пути Инициативой OpenNet, "Репортеры без границ" и, зачастую, использующими те же или аналогичные данные и классификации, Отчет о цензуре в интернете[[82]](#footnote-82).

Эти источники единогласно пишут об ошеломляющих масштабах процесса роста цензуры. Основываясь на их списках стран и цифрах, они приходят к выводу, что в настоящее время 1,72 миллиардов человек испытывают цензуру интернета. Это составляет 25,3% от нынешнего населения мира.

Список государств, где используется такая практика, довольно длинен, и в него входит, по крайней мере, 25, но, вероятно, более 30 – правительств, которые в значительной мере лишают своих граждан возможности доступа к полной информации, доступной он-лайн. В интернете есть несколько списков организаций, которые наблюдают за этими странами. Инициатива OpenNet делит их на Всеобъемлющие, Существенные, Номинальные и Косвенные, а также предлагает категорию Подозреваемых. Организация "Репортеры без границ" предлагает топ-лист 13 "Врагов интернета". В большинстве наблюдаемых стран вмешательство сосредоточено на запрете политического содержания  свобода, демократия, свободные выборы, средства юридической защиты, сообщения о сложных политических событиях – всем том, что не позволяет их собственная правительственная система, но многие идут намного дальше. Некоторые правительства сосредоточили свои ограничения на темах морали, традиционном моральном и культурном порядке. Интенсивность и тщательность контроля в разных странах различны. Есть несколько стран, в которых цензор блокирует страницы, но затем позволяет вызов поясняющей страницы, дающей доступ, если на экране отображается специальная "законная" информация, обеспечивая таким образом хоть какую-то степень прозрачности. В других странах цензура работает спорадически и неэффективно, и в случае нарушения блокировки санкции не применяются.

Однако как правило, правительственная цензура осуществляется без ограничений и распространяется на более широкий сегмент знания человечества, без какого-либо объяснения или юридического обоснования, даже в тех странах, которые в других отношениях являются вполне респектабельными: чем дальше страна от демократии западного типа, тем выше частота применения цензуры интернета посредством фильтрации. Некоторые государства стремятся учить свое население при помощи цензуры в интернете, доходя до определенных крайностей: интернет пользователи, которых уличили в доступе к запрещенным страницам, подвергаются наказаниям, а в некоторых странах их преследует агрессивная киберполиция. Число пользователей, попавших в тюрьму, даже то, о котором известно, вызывает тревогу с любой точки зрения. Некоторые международные ИТ-компании, поставщики программного обеспечения вынуждены жить с ощущением того, что они активно помогают и поощряют такие меры уголовного преследования, и тем самым способствуют вытекающим из них людским страданиям.

Последствия всеобъемлющей цензуры чрезвычайно серьезны, и их невозможно переоценить. Граждане не только ограничены в своих правах, обеспеченных международными законами, они также отрезаны от важнейших преимуществ информационного века, они имеют искаженный взгляд на мировую действительность, их участие в обогащающих процессах глобального общения снижается. Широкомасштабная фильтрация интернета может изменить общее состояние сознания нации. Следует также учитывать *двойное* негативное влияние этой цензуры: граждане лишены информации и возможности свободного мировоззрения, но цензура является также средством для политических репрессий, ограничивая свободу действия.

Такое положение дел, и ухудшение ситуации с цензурой интернета требует срочных действий. ЕС единогласно признал это и предпринимает действия. Он не признает, что компании, работающие в сфере IT-технологий, оказывают помощь репрессивным правительствам в укреплении их диктата над сознанием. Именно благодаря ЕС мы имеем сегодня весьма уместный термин "киберрепрессии" для обозначения этой практики.

ЕС действует не в одиночку. Международное лобби интернета, которое борется за свободу информации и целостность интернета во всемирном масштабе, также активно и бдительно действует, даже вне рамок многих уже упоминавшихся видных учреждений, которые наблюдают за развитием киберрепрессий и публично их порицают.

Учитывая способность опытных интернет пользователей избежать или обойти фильтрацию, многие международные защитники интернет свободы также участвуют в предоставлении гражданам стран, где применяется цензура, соответствующего противодействующего программного обеспечения, которое описано выше. Эта технология антифильтрации также превратились в настоящую отрасль промышленности, которая помогает снизить эффективность правительственной цензуры, не будучи в состоянии устранить ее полностью. Инициатива OpenNet, как и другие, активно действует в этой области, поставляя особенно эффективные системы, например Psiphon, предназначенные для работы в качестве личного зашифрованные проксисервера на обычном домашнем компьютере, обходя таким образом обязательным "брандмауэры", введенные правительством, и позволяя свободно передвигаться по глобальной сети. Однако применение этого устройства и других ему подобных встречает активное противодействие со стороны некоторых поставщиков фильтров. Это еще раз демонстрирует проблематичный характер коммерции многонациональных отраслей промышленности, которые – умышленно или в качестве нежелательного побочного ущерба, по сути, содействуют или помогают киберрепрессиям. Очевидно, следует добавить, что передовые страны в области цифровых технологий способны разрабатывать фильтры внутри страны, и многие уже это делают, что позволит отказаться от иностранных поставщиков программного обеспечения.

Как было подчеркнуто ранее, данная статья не претендует на детальный анализ для каждой страны, учитывая также и то, что интернет предоставляет на этот счет обширную информацию. Но даже краткое резюме, которое приводится здесь, и начавшееся общественное обсуждение поднимает вопрос о том, какие очевидно необходимые действия могут быть выполнены, что международная сообщество может сделать для противодействия киберрепрессиям как нарушению международных законов.

Правовые и политические проблемы, связанные с определением пределов для интернет фильтрации и возможных санкций, допустимых на международном уровне, очевидны, и они огромны. Вопросы национальной юрисдикции и суверенитета, невозможность определения реально действующей границы между гражданским свободами и важнейшими общественными интересами, вопросы выбора законов и средств правоприменения, и еще более широкомасштабный вопрос о регулировании интернета, *помимо прочего*, делают попытку создания международных кодексов нереализуемой и, вероятно, бесполезной. Существует также вопрос о культурном разнообразии, которое необходимо уважать. Определение культурного и религиозного *общественного порядка* не может быть единым для всех стран, хотя мы вправе предположить существование общих универсальных основных убеждений, и, в качестве общеобязательных должны рассматриваться Универсальная декларация и Пакты. Как и в большинстве международных законов, не бывает простых определений, и нет быстродействующих эффективных санкций.

Поэтому любая глобальная реформа интернет фильтрации должна рассматриваться *с точки зрения долговременного действия процессов и стратегий*. Надо рассматривать проблему как набор процедур, которые призывают мир к осознанию, способствуют привлечению общественного внимания и давления, и – для затронутых правительств – формируют вызов общественному мнению и мотивируют предоставление подробных обоснований.

Большая ответственность лежит на национальных правительствах, промышленности и организациях гражданского общества, имеющих, потенциал формирование убеждений. Правительства могут содействовать развитию и доступности технологий антифильтрации, могут подвергнуть экспорт технологий фильтрации соответствующим процедурам экспортного контроля, а также использовать национальные дипломатические средства для оказания давления на правительства, применяющие цензуру, заставляя их обеспечить прозрачность, открытость и законность своей ограничительной политики.

Предприятия ИТ-промышленности – производители программного обеспечения, компании, предоставляющие услуги доступа в интернет, и их объединения – несут очевидные обязательства и должны приступить к принятию кодексов поведения, которые исключили бы возможность использования их технологий для политической цензуры. Хотя в действительности никто не может потребовать от компаний, чтобы те полностью забыли о своих интересах, и было бы глупо перекладывать на промышленность главную вину за правительственную цензуру, добровольные совместные действия компаний также повлияет и на их репутацию и усилит их положительный имидж. Политика саморегулирования, обеспечивающая четкие общие стандарты, дала хорошие результаты в ЕС, она также может укрепить и силу сопротивления отдельных компаний, в противодействии давлению со стороны правительств, использующих цензуру, желающих сотрудничать с ними. Например, Инициатива "Глобальная сеть" добровольная организация технологических компаний США предписывает такие стандарты ("Хартия управления"), реагирует на просьбы правительства о цензуре, и продвигает свободу интернета[[83]](#footnote-83).

Академические институты и организации по правам человека, которые неустанно порицают киберрепрессии, ряд из которых назван выше, сегодня все чаще поощряют и поддерживают правительства, которых касается данная ситуация. Но, учитывая трансграничный и международный характер интернета, и глобальную значимость прав человека в ситуации с киберрепрессиями, самой важной задачей может состоять в том, чтобы включить этот вопрос в повестку дня международная организаций в совершенно новом свете.

Первый шаг мог бы состоять в достижении более широкого международного понимания развития и технической базы современной интернет фильтрации и в создании международного механизма ее мониторинга. На втором этапе можно было бы подумать о введении международной процедуры рассмотрения жалоб, доступной для всех заинтересованных сторон, а затем набора стандартов отчетности.

Какая международная организация или компания могла бы послужить такой борьбе?

Во-первых, можно было бы думать о Форуме по вопросам управления использованием интернета (IGF), созданном в 2006 году во исполнение решений ВВУИО ("Тунисской программы"). Ограничения, которые политическая цензура интернета накладывает на функционирование и управление Сетью, имеют очевидное значение для предназначения Форума, и могут быть легко включены в рамки его мандата (статья 72), б), д) и К) Тунисской программы), даже несмотря на то, что проблема киберрепрессий в этих текстах явно не упоминается. К сожалению, в течение пяти лет своего существования IGF ограничивался лишь обширными и значимыми дискуссиями, в том числе и о свободе интернета, но не начал никакой оперативной деятельности. Создание процедуры контроля, которая могла бы отслеживать анализировать и критически оценивать применение методов фильтрации, могло бы соответствовать условиям Форума, если его мандат будет расширен, что представляется вполне вероятным, возможным и

желательным[[84]](#footnote-84). Ежегодный форум ВВУИО, напротив, представляет собой открытый дискуссионный форум без оперативного назначения, и подходит для этой цели в гораздо меньшей степени.

Организация ЮНЕСКО в соответствии с актом о ее создании, с гордостью провозгласила себя уникальным международным защитником свободы информации, и получила от ВВУИО четкие задачи с общими заголовками "Доступ к информации и знаниям" и "Этические аспекты интернета". ЮНЕСКО принимает Декларации и Рекомендации, которые обязуют государства-члены и международные организации обеспечить свободный и неограниченный доступ к интернет[[85]](#footnote-85), и ее Генеральный директор постоянно публично осуждает нарушения свободы информации и прессы. Ничто не было бы более логичным, чем приступить к диалогу для выполнения этих задач и, как результат, периодически рассматривать случаи цензуры.

Поскольку мы имеем дело с правами человека и две основные международные конвенции провозглашают обязательства государств в отношении этих прав, главным местом проведения международных действий должны стать специальные организации по правам человека в рамках Организации Объединенных Наций, Совет по правам человека, учрежденный в 2006 году, и специальный орган для борьбы с нарушениями *Международного пакта о гражданских и политических правах*. Совет по правам человека с его широкими полномочиями получит право ввести в действие процедуру официального рассмотрения жалоб, доступную для правительств всех государств членов ООН. Одной из возможностей будет также обязательное включение темы о свободе и цензуре интернета в процесс всеобщего периодического обзора, согласно которому оценивается обеспечению прав человека в разных странах. Вне зависимости от выбранной процессуальной формы, общее освещение нарушений прав человека в этой сфере может формировать необходимое давление и необходимость оправдываться для правительств, подозреваемых в нарушении законности. В рамках процедуры рассмотрения жалоб также может быть адекватно рассмотрена сомнительная роль международной ИТ-индустрии в создании инструментария для киберрепрессий. Поскольку СПЧ периодические готовит обзоры стран для Комитета по правам человека ООН, в них могли бы также включаться и аспекты свободы интернета.

Однако насколько простыми не были бы такие процедуры, прозрачный режим "соблюдай или объясни", приводящий, в конечном итоге, к общественному давлению и общественному осуждению, на самом деле мог бы проложить путь к более глобальной осведомленности о данной проблеме, и, в конечном итоге, к оптимизации ситуации в цифровом мире.

# 5 Киберконфликт и геокиберстабильность

## 5.1 Киберконфликт

**Джанкарло А. Барлетта (Giancarlo A. Barletta**[[86]](#footnote-86)**), Вильям А. Барлетта (William А. Barletta**[[87]](#footnote-87)**), Виталий Н. Цыгичко (Vitali N. Tsygichko**[[88]](#footnote-88)**)**

Введение: Природа проблемы

Информационная война так же стара, как человеческий конфликт. Мотивы их мало изменились, они включают в себя подрыв доверия к противнику, повреждение и нарушение линий связи противника, а также создания иллюзий относительно характера и состояний конфликта. Эти мотивы остались неизменными. Что же является совершенно новым в XXI веке, во времена всеобщей электронной информационной инфраструктуры с постоянно расширяющейся высокой пропускной способностью цифровых линий связи, это: а) болезненность и частота информационных атак, которые могут разрушить социальную основу атакуемой страны; b) далеко идущие возможности по созданию обширных физических повреждений; с) потенциальное заражение и возможность осуществления устойчивых информационных атак, открытая для неправительственного сектора и даже для частных лиц, которые могут теперь участвовать в асимметричных боевых действиях, и d) создание основного состояния в виде вечно длящегося распространенного конфликта на низком уровне, что можно назвать холодной кибервойной. Интенсивное внедрение новых информационных технологий значительно увеличило боевые возможности обычных вооружений и другой военной техники. По этой причине, военные теперь рассматривают информационные и коммуникационные технологии (ИКТ) и в качестве оружия, и в качестве цели, и видят киберпространство как территорию для военных действий, аналогично воздушному пространству, космосу, суше и морю[[89]](#footnote-89).

За последние два десятилетия промышленно развитые страны развернули широкомасштабные сети, которые с помощью ИКТ связали основные экономические, физические и социальные активы, с целью повышения уровня жизни, экономического процветания, международного влияния и могущества. Развивающиеся страны также рассматривают информационные технологии в качестве ускоренного экономического пути к полномасштабному участию в глобальной экономике. В нашем распоряжении имеется множество интеллектуальных устройств для промышленности, содержащих датчики и микропроцессоры, а также потребительских устройств с микропроцессорами, и, кроме того, беспроводные или сотовые технологии, такие как мобильные телефоны, КПК и электронные записные книжки. Обширные сети связи дают возможность интенсивного использования информационных ресурсов для торговли, предоставления услуг, мониторинга окружающей среды и решения сложных социальных проблем. Все эти устройства быстро развивается, и обладают возможностью связи с другими устройствами в любой точке земного шара.

Как отмечает бывший генерал вооруженных сил США, те же самые ИКТ, которые связывают основные экономические, физические и социальные активы, были приняты и адаптированы военными и полувоенными организациями, способствуя революционным преобразованиям в военном деле, изменив способ планирования, организации и ведения боевых действий. Эта "революция" включает в себя достижения способности проведения разведки, наблюдения и рекогносцировки, командования и управления силами и их действиями; для оптимизации движения транспорта; для обеспечения точности навигации и применения "интеллектуального" оружия. Очень важно, что они позволяют также использовать "сеть" в качестве среды, из которой, при помощи которой и в рамках которой проводятся военные операции[[90]](#footnote-90).

Информационные технологии продвигают и содействуют новым отношениям в обществах с природным потенциалом для повышения экономического роста, обеспечения прав человека и выявления государственных репрессий. Национальные органы управления пользуются значительно облегченными средствами связи "сверху вниз", но, что более важно, с целью расширения прав человека и экономического благосостояния, информационные потоки "снизу вверх" и горизонтальные информационные потоки превращаются в огромные реки. Современные информационные общества постоянно увеличивают количество и атрибуты информационных узлов, в которых информация создается и потребляется, а также количество и пропускную способность каналов связи. Кроме того, все больший процент узлов и каналов содержит автономные датчики своей готовности.

Такие высоко нелинейные подключения увеличивает одновременно как устойчивость информационной сети, так и риски, и последствия изнурительной атаки на узлы и магистральные каналы связи, а также трудности в прогнозировании последствий сбоев в работе сети. Быстрое развитие ИКТ и последующая эволюция глобального информационного общества способны породить широкий спектр негативных геополитических последствий: ускорение глобальной поляризации между богатыми и бедными странами, расширение технологического разрыва между промышленно развитыми и развивающимися странами, оставляя все больше экономически изолированных стран на обочине эволюционного развития цивилизации, создавая основной источник политической нестабильности и конфликтов. Следовательно, с органическим ростом сложности информационных сетей, эволюционирует и возможность информационных войн, и путь этого развития направлен в сторону повышения риска для социальных ценностей.

Общественный запрет на кибератаки против кибервойны правительств

Атаки на компьютерные сети, системы и цифровые данные привели к принятию во многих странах законов о киберпреступности. Хотя в большинстве промышленно развитых стран имеется тот или иной закон киберпреступности, значительные различия в определении того, что является киберпреступностью, в выявлении и определении преступного поведения в киберпространстве, а также в применимых материально-правовых и процессуальных положениях ставит значительные препятствия на пути международного сотрудничества в области содействия раскрытию преступлений. Конвенция о киберпреступности Совета Европы (СоЕ) была разработана в качестве многостороннего соглашения, которое должно было послужить началом гармонизации глобальных законов о киберпреступности. Однако реальность не оправдала ожиданий, к середине 2010 года, почти через девять лет после того, как она была открыта для подписания, Конвенцию ратифицировали только 26 стран. В качестве альтернативного более гибкого пути был разработан Инструментарий МСЭ для законодательства о киберпреступности, он содержит образца языка законодательства, гармонизированного с Конвенцией Совета Европы и законами о киберпреступности промышленно развитых стран, и может быть использован странами всего мира для разработки и внесения изменений в свои собственные законы о киберпреступности.

Другие законы, относящиеся к определенным видам кибердеятельности, включают законы, защищающие физические системы и оборудование поставщиков услуг связи, регламенты, запрещающие действия экономического шпионажа, законы об интеллектуальной собственности и т. д. В целом, эти законы предназначены для обеспечения юридического запрета кибератак различного рода против инфраструктур, систем и данных любого типа.

Широкий спектр возможностей с каждым днем становится еще шире, появляются более мощные и более всепроникающие информационные технологии. Неудивительно, что страны мира стремятся узаконить правила поведения в киберпространстве, вне зависимости от своего собственного поведения по отношению к другим странам. Поскольку информационные технологии могут легко пересекать международные границы, преступникам нет необходимости физически находиться в той же стране, что и их жертва. Следовательно, появляются большие стимулы для сотрудничества между государствами, особенно, учитывая, что привлекательной мишенью для преступных действий являются государственные информационные ресурсы. Отсюда, сотрудничество как в пропаганде плодотворного взаимодействия с использованием информационных сетей, так и в предотвращении или, по крайней мере, сдерживании преступлений в киберпространстве серьезно беспокоит такие международные организации, как МСЭ.

Так как правительства все больше полагаются на интернет, как средство упрощающее распространение информации и предоставление услуг для своих граждан, информационное общество представляет собой заманчивую цель для злоумышленников, будь то преступники, субнациональные террористические группы или враждебные государства. Атака[[91]](#footnote-91) на национальную информационную инфраструктуру Эстонии в апреле 2007 г. явно показывает, как предсказанную уязвимость электронного правительства, так и отсутствие факторов, которые могли бы остановить злоумышленника. Многие эксперты утверждают, что техническая изощренность атак превышает все ранее известные случаи. Хотя некоторые идут еще дальше, заявляя, что для такой атаки требовались знание или сговор с национальной государственной организацией, некоторые эксперты США сбрасывают такие размышления со счетов. Однако эстонская ситуация не сопровождалась политическими или финансовыми требованиями или заявлениями со стороны предполагаемых лидеров этой атаки[[92]](#footnote-92), делает маловероятным преступление без политической мотивации. Другие примеры более устойчивых и более обширных кибератак описаны как атаки GhostNet[[93]](#footnote-93) и Aurora в 2009 году. Один из аспектов атаки был сосредоточен на серверах Google, и проводился, по-видимому, в рамках согласованных действий политического и корпоративного шпионажа, которые "использовали бреши безопасности во вложениях сообщений электронной почты, для того чтобы проникнуть в сети крупных финансовых, оборонных и технологических компаний, а также и исследовательских институтов Соединенных Штатов"[[94]](#footnote-94).

Как показывает эстонский инцидент, интенсивные и устойчивые кибератаки могут *де‑факто* представлять собой прямое и мощное нападение на гражданские и государственные структуры, уровень которого превышает простую преступность. Для таких атак могут быть характерны: а) серьезные физические повреждения критически важных объектов, b) широкомасштабные травмы или гибель людей, с) беспорядок в финансовых учреждениях; и в) нарушение работы критической инфраструктуры. Если такие атаки скоординированы или ведутся непрерывно в течение длительного периода, то тяжести их последствий, скорее всего, умножатся. В таких обстоятельствах, вне зависимости от того, известны ли личности или мотивы нападающих, государства могут рассматривать[[95]](#footnote-95) обширные кибератаки как акт терроризма или функциональный эквивалент вооруженного нападения, что оправдывает особое внимание к ним и специальные действия для исправления ситуации.

По крайней мере, продемонстрированные возможности крупномасштабных нарушений работы информационного общества требуют формирования основ культуры взаимного сотрудничества по каналам связи отдельной страны. В эстонском примере первая волна нарушений работы правительственных сайтов привела в движение планы реагирования, которые строились в ожидании волны нападений на финансовые услуги, такие как он-лайн-банкинг. На самом деле, в течение нескольких дней "частные банки и интернет-СМИ также подверглись нападению, и атаки нарушили работу остальной части сетевой инфраструктуры в Эстонии"[[96]](#footnote-96). В этот же период совместно с поставщиками услуг интернета по всему миру были предприняты контрмеры, расширившие блокировку трафика, исходящего с IP-адресов указанной группы, и защитить эстонскую банковскую систему от всего международного трафика. Следует отметить, что сеть ресурсов, потребовавшихся для устранения последствий кибератаки, должны были во много раз превысить ресурсы, используемые для осуществления атак.

Значительная асимметрия между преступлением и обороной в киберпространстве не остается незамеченной. Незнакомые с атаками такого масштаба, военные и разведывательные учреждения США и других государств (Россия, Китай, Индия, Пакистан, Иран), уже "разведывают и зондируют цифровые сети потенциальных противников для выявления слабых мест". Лица, принимающие решения в этих странах, действуют так, как если бы сейчас началась эпоха киберконфликтов. На самом деле, именно такие страны, как США, которые имеют асимметричный потенциал и возможности для осуществления или финансирования кибератак, особенно в виде тайной операции, против стран, которые в меньшей степени способны ответить тем же. Более того, власти в этих и других странах хорошо знают, что большая асимметрия наступления-обороны в сочетании с почти полной анонимностью злоумышленников дает возможность прямого или опосредованного использования малых "армий" кибернаемников или "незаконным бойцов", которые обеспечат властям государства возможность правдоподобно отрицать свою сопричастность.

На практике, потенциальная опасность данной атаки может значительно меняться в зависимости от степени готовности общества и встроенной безопасности атакуемой инфраструктуры. С точки зрения политических или военных официальных деятелей "важным вопросом в борьбе с любой формой кибератаки является возможность быстро распознать тип атаки и противника, а затем ответить надлежащим образом. В настоящее время, расследование проникновений в компьютер является функцией правоохранительных органов. ... Традиционным военным, ведущим боевые действия, запрещено выполнение этих задач внутри страны ... [следовательно] важную роль в обеспечении национальной безопасности и национальной обороны играют правоохранительные органы страны"[[97]](#footnote-97). Отсюда следует, что государствам в обоих своих органах – военных и правоохранительных – требуется иметь мощные цифровые инструменты судебной экспертизы и соответствующие законные структуры для их применения, надежных способы сохранения целостности доказательств и наказания для преступников, которые имеют реальные возможности сдерживания. Так как эти инструменты имеют сильный потенциал "двойного назначения", те страны, которые приобретут самые сильные и гибкие возможности для обороны и судебной экспертизы, получат в свои руки, *еще более,* значительные возможности для атак и возможности кибершпионажа. Хотя в области физической оружия также присутствуют асимметрия и потенциал двойного использования для преступления и для обороны, вероятность физической атаки снижена (хотя и не устранена окончательно) концепцией сдерживания и относительной легкостью определения источника атаки.

Взаимодействие информационного и физического конфликтов

Интенсивное внедрение новых информационных технологий одновременно укрепляет, и повышает боевые возможности вооружения и военной техники. Информационные технологии позволяют качественно изменить военную и разведку и связь. Они значительно повышают скорость обработки огромных массивов данных и принятия сложных оперативных решений, что делает возможным перейти к принципиально новым методам управления войсками и вооружениями на всех уровнях от стратегического до тактического. Новые информационные технологии резко повышают боевой потенциал электронных вооружений и создают новый тип оружия, в частности, информационное оружие, предназначенное для повреждения военных и гражданских информационных инфраструктур противника, путем повреждения его компьютерных сетей.

Для военных информационная и технологическая революция резко увеличивает боеспособность войск, не только меняя формы и методы боевых действий различных масштабов, но меняя традиционную парадигму вооруженной борьбы и эскалации конфликта. По данным американских экспертов, информационное оружие, избирательно нацеленное на критические военные и гражданские информационные инфраструктуры противника, может прекратить конфликт до начала физических боевых действий сторон, тогда как эскалация результатов информационной приведет к катастрофе. Обладание информационным оружием обеспечивает подавляющее преимущество над странами, его не имеющими. Если не сегодня, то в ближайшем будущем, информационные и политические переменные противостояния властей будут доминировать над ядерными. В отличие от ядерного противостояния, для информационного оружия уязвимы все страны, особенно высокоразвитые. Информационное оружие, как и ядерное, может служить фактором политического давления и устрашения.

Информационная война – это не виртуальная реальность компьютерных игр, а вполне осязаемый инструмент достижения победы в военных или политических конфликтах. Без сомнения, информационное оружие становится основным компонентом военного потенциала нации, и многие страны, в частности, США и Китай, настойчиво и активно готовится к ведению информационных войн.

Природа информационного оружия

Концептуальная проблема формулирования парадигмы информационной безопасности заключается в определении и выявлении "информационного оружия". Каковы отличительные особенности информационного оружия? Какой (если таковой имеется) уровень киберконфликта должны считаться вооруженным конфликтом? Отсутствие какого-либо международного консенсуса в отношении этих вопросов препятствует началу конструктивных переговоров по глобальной информационной безопасности. Один из подходов к определению концепции "информационного оружия" опирается на его способность воздействовать и на военные, и на гражданские информационные инфраструктуры[[98]](#footnote-98). Недостатком такого подхода является то, что любой вид оружия, включая обычное, если оно способно повредить компоненты информационной инфраструктуры можно назвать информационным оружием. Например, не все ли равно, какое устройство вывело из строя систему управления коммунальным хозяйством  программный код, мощный электронный импульс или прямое попадание обычного взрывчатого вещества? Второй подход может состоять в том, чтобы назвать информационным оружием все средства поражения, в которых используются ИКТ.

Чего требуется избегать в вопросах киберконфликта, так это  снижение барьера признания войне, принимая определения, включающие действия, часто выполняемые

в мирное время. Каковы отличительные особенности информационного оружия? Какой уровень киберконфликта следует считать вооруженным конфликтом? Было бы неразумно и опасно для международной стабильности считать "вооруженными конфликтами" конфликты, которые не несут явных угроз для жизни человека или социальных свобод. Кроме того, поскольку практически во всех сложных системах вооружений, где используются ИКТ, чрезвычайно трудно, если вообще возможно, выделить информационное оружие из всего спектра вооружений. Так как информационная война является постоянным явлением в истории человеческих конфликтов, ей особенно трудно дать четкое определение в присутствии нескольких уровней концептуальной сложности. Например, как следует классифицировать предоставление заведомо неверной информации? Что сказать о шпионаже или перехвата информационных потоков? Если бы такие действия были обнаружены во время физической войны, то перспективы, для того что их совершил, были бы совершенно ясны.

Важными эксплуатационными характеристиками информационного оружия являются: 1) его относительно низкая стоимость и доступность; 2) возможность скрытой разработки, накопления и внедрения; и 3) присущая ему экстерриториальности и анонимность воздействия. Эти функции позволяют неконтролируемое распространение информационного оружия и делают его владения агрессивными режимами опасной глобальной проблемой. Обусловленная таким оружием угроза международному миру и стабильности призывает мировое сообщество контролировать угрозы для информационной безопасности национальной и глобальной инфраструктур, осуществляя практических шагов в направлении нейтрализации киберугроз. Будучи частью инфраструктура современного общества, ИКТ входит в набор инструментов государства для борьбы с врагами. Многие страны принимают меры для противодействия угрозам информационной безопасности, однако эффективность даже жестких мер уменьшается из-за транснационального характера угрозы и анонимности преступников. В таких условиях ни одна страна не может быть в безопасности, если пытается противостоять информационным угрозам в одиночку. Только создание международного режима информационной безопасности и согласованные усилия всех его участников может сдержать распространение информационного оружия и снизить угрозы информационной войны, информационного терроризма и киберпреступности.

Информационным оружием, как минимум, можно однозначно назвать программное обеспечение, предназначенное исключительно для уничтожения информационной инфраструктуры (различные вирусы, закладки и т. д.). Большинство сложных средств вооруженной борьбы, использующих ИКТ, являются многофункциональными, т. е. предназначенными не только для уничтожения информационной инфраструктуры, но и для других боевых задач. Страны, обладающие такими современными системами вооружений, средств разведки, связи, навигации и управлении, которые в широком масштабе применяют ИКТ, могут похвастаться решающим военным преимуществом, а значит, они вряд ли когда-нибудь вступят в соглашения, ограничивающие их стратегические преимущества.

Следовательно, сама проблема запрещения или ограничения производства, распространения и применения информационного оружия, вероятно, будет ограничена оружием одной цели, предназначенным только для поражения компонентов информационной инфраструктуры, например, оружием, основанным на программных кодах, т. е. различных вирусах и средствах их доставки. К сожалению, подавляющее большинство современных ИКТ, которые могут использоваться в военных, террористических и преступных целях, разрабатывается в гражданских отраслях промышленности; таким образом, очень трудно контролировать их разработку и распространение.

Угрозы, создаваемые инструментами для киберконфликта и информационной войны, является реальными для всех, особенно для развитых стран, где вся жизнедеятельность определяется комплексом информационной инфраструктуры[[99]](#footnote-99). Только совместными усилиями международного сообщества по обеспечению безопасности важнейшей национальной информационной инфраструктуры, можно снизить угрозы злоумышленного использования информационных технологий. Консенсус относительно этого класса информационных систем позволит реализовать более эффективные меры сдерживания, а также более эффективные меры защиты, в том числе право на осуществление ответных действий в случае информационных операций против них, которые оказывают серьезное, неприемлемое прямое воздействие. Даже здесь требуется крайняя осторожность. Инициирование физической войны не моет быть оправдано только каким-либо агрессивным информационным действием; было бы неразумно давать правительствам права принимать самостоятельные решения о ее начале.

Ограничение киберконфликта

Возможная значительная асимметрия между наступательными и оборонительными информационными технологиями приводит к состоянию, в котором конечные пользователи могут вести личные "кибервойны" против важнейшей информационной инфраструктуры общества с почти такой же силой, что и другие государства. Следовательно, правовой и политический режим сдерживания и ограничения киберконфликтов между странами будет де-факто связан с правовой и процедурной основой сдерживания и противодействия кибертерроризму и киберпреступности.

В реалиях информационного общества концепция сдерживания посредством гражданского и уголовного наказания может регулироваться на уровне преступности или "хактивизма"[[100]](#footnote-100), если может быть достигнута требуемая международная однородность в уголовных кодексах. К сожалению, на уровне кибератаки государств, концепции сдерживания, разработанные во время холодной войны, могут иметь очень небольшую ценность, так как физическая контратака может разрушить международные социальные и физические контакты на таком уровне, который является неприемлемым и для третьих сторон, и для того, кто противостоит злоумышленнику. В киберпространстве этот побочный ущерб может быть всемирным, он может многократно повторяться при быстром распространении таких вредоносных программ, как компьютерные вирусы. В промежуточном случае кибертерроризма, учитывая недавнее поведение Соединенных Штатов в отношении "незаконных бойцов" в их "войне с терроризмом", можно предположить, что и здесь модель сдерживания на уровне гражданского и уголовного наказания не сработает.

В то время как трудность сдерживания может стимулировать создание совершенной технологической защиты от кибератак, история любого другого вида оружия предупреждает, что в конечном итоге то, что лежит в основе социально-политических проблем следует рассматривать на социально-политическом уровне. С политической стороны, серьезная возможность международного киберконфликта требует немедленного внимания. Двойственный характер использования технологии исключает применение международного режима контроля, используемого для регулирования ядерной технологии. То, на что можно надеяться на (и над чем работать) это – создание транснациональной правовой базы, которая установит правила и меры наказания за киберконфликт в виде комплекса структурированных, согласованных на международном уровне обязательных соглашений. Такие правила должны устанавливать обязательства подписавших их стран в отношении контроля неправительственных организаций или сетей, которые физически действуют в пределах государственных границ.

Хотя по закону атаки кибертеррориста или кибершпионажа в целом могут быть рассматриваться по общему уголовному гражданскому законодательства и связанным с ними юридическими положениями, некоторые их характеристики могут требовать специальных законов, что само по себе приводит к специальным юридическим положениям. Эти характеристики могут включать: 1) широкомасштабный ущерб с политическим подтекстом, 2) повышенные трудности в выявлении, захвата и уголовного преследования виновных; и 3) наличие сильной политической мотивации, направленной на дестабилизацию общества в нарушение общепринятых понятий как уголовного право, так и законов вооруженного конфликта. Существует дополнительный аргумент для специального обращения с кибертерроризмом. "Особые ответные меры, как правило, могут быть оправданы, когда угроза терроризма исходит от группы, имеющей возможность организовать коллективное, на постоянной основе, осуществление сложных планов и операций и работать независимо от нормальной жизни, или имеющей возможность запугивать нормальное общество, заставляя терпеть свое присутствие[[101]](#footnote-101)." Затянувшийся киберконфликт, проводящийся в террористических или военных целях, может потребовать или стимулировать скоординированные международные действия для ограничения или контроля применения силы.

Эффективный режим управления также должен законодательно определить действия, которые могут предприниматься в отношении негосударственных нападающих, если их, реально можно идентифицировать. В случае террористического акта, осуществляемого в стране, которая подверглась нападению, действия в отношении злоумышленников могут быть осуществляться в рамках существующего национального уголовного права, в том числе антитеррористических положений. В случае атак, осуществляемых со стороны сотрудничающих или нейтральных государств, имеется несколько вариантов: 1) экстрадиция преступника в атакованное государство, 2) вынесение обвинения в нейтральной стране, с территории которой осуществлена атаки; или 3) выдача преступника третьей стороне, которая имеет универсальное законодательство и общепринятые процессуальные правила. Вопрос о том, какой из вариантов принять, решается из баланса соображений, касающихся участия государства источника атаки, требований правосудия и укрепления международной нетерпимости к террористическим методам.

Осуществление кибератаки из изолированной или отказавшейся от сотрудничества стран исключает возможность применения странами нормальных каналов взаимодействия в расследовании случая атаки, задержания и судебного преследования, или, в соответствующих случаях, экстрадиции виновных. Главным вопросом является то, будет(ут) ли преследоваться злоумышленник(и) будет в стране, которая пострадала от атаки, в нейтральной третьей стране или в Международном уголовном суде. Следовательно, такие случаи естественно переходит в вопросы о силовом вмешательстве или международных санкций. Эти вопросы должны рассматриваться параллельно со случаями терроризма, осуществляемого физическими средствами. Для страны, которая пострадала от атаки, открыты следующие возможности

1 ответные действия в отношении этой страны;

2 несанкционированное проникновение и задержание[[102]](#footnote-102) подозреваемых в правонарушении, а также

3 должное уважение к суверенитету за счет привлечения стороннего государства-посредника.

Если бы можно было представить себе режим, в котором некоторые классы действия в киберпространстве были бы запрещены по аналогии с Женевской конвенцией относительно физической войны, то можно было бы предположить и случай универсальной юрисдикции, в которую входит международная группа. Такая возможность создает скользкие аргументы по отношению к общему беззаконию в интернете и его подавлению. Отметим, что Конвенция о киберпреступности Совета Европы не может определить киберпреступность и, следовательно, не дает никаких оснований для трансграничного поиска доказательств по компьютерным сетям, даже по горячим следам.

**Заключительные замечания**

Признанными фактами являются: 1) в большинстве стран бизнес, правительства и коммунальные услуги сильно зависят от компьютеров и интернета; 2), хотя интернету присуща устойчивость в отношении соединений, компьютеры, которые присоединены к интернету, намного более уязвимы для нападений; 3) для приобретения довольно мощные средств для атаки в настоящее время не требует значительных инвестиций, и 4) очень трудно выявить точный источник атаки.

Что касается законов войны, большинство стран могло согласиться на некоторые общие принципы в качестве основы для гармонизированного порядка в киберпространстве.

1 Кибератаки на важнейшую инфраструктуру не является законным оружием для нападения даже во время физической войны. Аналогами являются биологическое и химическое оружие.

2 Проникающий, оплаченный правительством интернет-шпионаж затрудняет выявление вторжений и нарушений со стороны организованной преступности, субнациональных организаций и хакеров, и это мешает уголовному преследованию этих групп в соответствии с законами о компьютерных преступлениях.

3 Низкий уровень компьютерного шпионажа со стороны правительства может быть приемлем, но саботаж не допускается. Невысокий уровень "конкуренции" пришпоривает технический прогресс. Кроме того, каждая страна желает знать, что безопасность иностранных военных систем находится в целости и сохранности от атак со стороны потенциальных злоумышленников.

4 Правительство, ведущее шпионаж за иностранными частными компаниями, имеет неясное, но, вероятно, небольшое реальное влияние в мире. Тем не менее, такой шпионаж вызывает нездоровый националистический пыл у граждан, создает нежелательные сигналы для промышленности и, если это выполняется от страны, ее собственная промышленность стремится к получению экономического могущества без конкуренции.

5 Поскольку очень трудно определить источник атаки и того, финансируется ли он правительством, национальный конфликт могут быть спровоцировать почти любые злонамеренные неправительственные организации.

Поскольку проверить официальные соглашения может быть невозможно, первоначальная цель международного диалога может состоять в том, чтобы установить правила предоставления доказательств, необходимых для соблюдения правил честной игры. В этом свете представляются, что утверждения об экономическом преимуществе или основной политической динамике подразумевает динамику типа Холодной войны, что подрывает сами цели, которых стремится достичь международное соглашение[[103]](#footnote-103). Еще более важно, если это  правда, то никакое соглашение ООН не в силах остановить этот процесс.

Двигаясь к цели смягчения киберконфликта, новую информацию для политических дискуссий, проводящихся в международных центрах, будут давать дальнейшие исследования в следующих областях:

1 теоретическая динамика нападения/обороны компьютерной безопасности,

2 динамика нападения/ обороны компьютерной развития безопасности как вопрос возврата инвестиций;

3 влияние, которое надежные системы безопасности оказывают на работу компьютерной обработки, хранения данных, систем управления, время действия интерфейса человек-машина),

4 стимулы и сдерживание правонарушений в трансграничной преступности,

5 воздействие компьютерного шпионажа на государственный и частный сектора.

## 5.2 Призыв к геокиберстабильности

**Джоди Р. Вестбай (Jody R. Westby)**

Скорость, с которой растет киберпреступность, не может быть устойчивой. Используя ботнеты, мошенники обычно добывают конфиденциальную и служебную информацию, и осуществляют распределенные атаки типа "отказ в обслуживании" против правительственных и коммерческих систем. По оценкам из отчета компании McAfee 2009 года "Незащищенные страны: Защита жизненно важной информации", в 2008 году респонденты потеряли интеллектуальной собственности в общей сложности на сумму 4,6 млрд. долларов США и потратили около 600 миллионов долларов на возмещение ущерба от утечки данных. На основании этих цифр, McAfee прогнозирует, что в 2008 году компании по всему миру потеряли более 1 трлн. долларов США. Люди вынуждены постоянно обновлять программное обеспечение операционных систем и антивирусных программ, и все равно многие их системы заражены и используются для осуществления атак.

Страны признают, что их правительственные и коммерческие системы являются ценными, и что их национальная и экономическая безопасность подвергаются риску. Поэтому они приступили к разработке стратегий кибервойны и создают киберкоманды, имеющие возможность наступления и обороны. Хотя такие действия необходимы и ожидаемы, существует заметный вакуум в отношении диалога о кибермире, а тем более о поддержании приемлемого уровня геокиберстабильности. Как отмечается во Введении, автор определяет "геокибер" отношения, как взаимосвязь интернета с географией, демографией, экономикой и политикой страны, а также ее внешней политикой. "Геокиберстабильность" определяется, как способность всех стран использовать интернет для получения экономических, политических и демографических преимуществ, в то же время, воздерживаясь от действий, которые могли бы причинить излишние страдания и разрушения[[104]](#footnote-104).

В частности, нежелание стран принимать участие в дискуссии о том, какие "минимально необходимые коммуникации" требуются для защиты жизненно важных общественных функций и предотвращения ненужных страданий и разрушений, вызванных кибератаками, может вытекать из общей неопределенности относительно того, каким образом такой вопрос может быть рассмотрен в рамках современное международной правовой базы.

Законы вооруженного конфликта

На протяжении всей современной истории, международные законы вооруженного конфликта (LOAC) обновлялись в ответ на зверства войны и появление новых методов ведения военных действий. В настоящее время назрела настоятельная необходимость сделать это еще раз, для того чтобы привести их в соответствие с кибервозможностями, потому что боевые действия кибервойны, скорее всего, либо нарушают многие положения существующих законов вооруженного конфликта или выходят за рамки всех законов.

Основные правовые рамки, касающимися вооруженных конфликтов, являются обширными и в основном были разработаны в прошлом веке. Основные документы, имеющие отношение к киберконфликту, включают в себя:

• Хартию Организация Объединенных Наций[[105]](#footnote-105)

• Североатлантический договор (НАТО)[[106]](#footnote-106)

• Женевская конвенция 1949 года[[107]](#footnote-107)

• Женевский Дополнительный протокол к Женевской конвенции от 12 августа 1949 года, касающийся защиты жертв вооруженных международных конфликтов (Протокол I)[[108]](#footnote-108)

• Гаагские конвенции (1899 и 1907 годов)[[109]](#footnote-109)

• Конвенции о запрещении или ограничении применения определенных видов обычного вооружения, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие[[110]](#footnote-110).

Основные положения этих документов могут быть упрощены. Законы вооруженного конфликта регулируют проведение военных действий, и военные должны планировать и осуществлять свою деятельность в рамках этих законов. Они применяются к военным операциям и связанным с ними видам деятельности и предназначены для предотвращения ненужных страданий и разрушений во время войны. Специальные положения защищают гражданских лиц, заключенных, больных и раненых, и потерпевшие кораблекрушение.

Как могут проводиться военные действия

Существует три основных принципа, регулирующих то, *как* военные действия могут быть проведены: необходимость, различие, и соразмерность.

*Необходимость*: Принцип необходимости ограничивает использование вооруженных сил только теми действиями, которые необходимые для достижения законных военных целей. Военные объекты, оборудование и силы могут быть направлены, если это приведет к частичному или полному подавлению противника.

*Различие:* Принцип различия требует, чтобы военные различали законные и незаконные цели, такие как гражданские, гражданские объекты и раненые. Гражданские объекты должны быть в максимально возможной степени отделены от военных целей. Нападениями неизбирательного характера считаются те, которые нацелены как на военные, так и на гражданские объекты, военных и граждан.

*Соразмерность*: Принцип соразмерности запрещает использовать силы сверх того, которые необходимы для достижения военных целей. Этот принцип сравнивает военное преимущество, достигнутое в ходе атаки, с причиненным вредом, и требует равновесия между непосредственным военным преимуществом, и ожидаемыми повреждениями или ущербом для гражданских лиц.

Кто может проводить вооруженный конфликт

Участвовать в вооруженных конфликтах могут только *законные бойцы*. Законные бойцы  это лица, уполномоченные правительством на участие в военных действиях. Это могут быть нерегулярные силы, но они должны быть под командованием лица, ответственного за подчиненных, иметь отличительные эмблемы, узнаваемые на расстоянии, например, по форме или цвету, открыто носить оружие, а также проводить операции в соответствии с LOAC

*Незаконными бойцами* являются те, кто принимают непосредственное участие в военных действиях без разрешения правительственных властей или международная права. Примерами незаконных бойцов являются гражданские лица, нападают на войска, пираты и террористы.

*Мирное население* – это лица, не уполномоченными правительством на участие в военных действиях, но участвуют в них. В эту группу входят такие лица, как священники, гражданский персонал, сопровождающий военных, а также медицинский персонал. Мирное население не может быть объектом прямого нападения, но в случае прямой атаки эти люди могут быть убиты.

Если статус бойца неизвестен, то применяется Женевская конвенция до тех пор, пока статус человека не будет определен.

Что может являться целью

*Военные цели* это  цели, которые, в силу своего характера, расположения, назначения или использования эффективно усиливают военные возможности противника, чье и полное или частичное уничтожение или нейтрализация в момент атаки является достижением законных военных целей.

*Охраняемые цели* это – цели, защищаемые Женевской конвенцией, таких как больницы, транспортировка раненых и больных, религиозные или культурные объекты и зоны безопасности. Однако если какие-либо из этих целей используются в военных целях, они могут быть атакованы. Например, если военные использует церковь в качестве базы для операций, она становится законной военной целью[[111]](#footnote-111).

В контексте кибервойны эти принципы ставят некоторые нерешенные вопросы:

• Что представляет собой действие в рамках вооруженного киберконфликта?

• Может ли быть целью важнейшая инфраструктура?

• Если важнейшая инфраструктура поддерживает цели, которые находятся под защитой Женевской конвенции, могут ли эти сети быть целью?

• Необходимы ли атаки на важнейшие инфраструктуры для достижения военных целей?

• Каким образом смогут участники военных действиях отличать цели военные от защищаемых?

• Соответствует ли повреждение важнейших инфраструктур достижению военных целей?

• Что такое чрезмерная сила в киберпространстве?

• Как отличить киберсолдат?

• Как то определить ситуацию, когда за государство действуют третьи лица?

В соответствии с существующим законом ни на один из этих вопросов нет ясного ответа. Например, являются ли частные сети связи США законной военной целью, и входят ли в число сетей военной необходимости, поскольку правительственные сетей связи США на 90% используют коммерческие сети, включая интернет, телефонию, сотовую и спутниковую связь[[112]](#footnote-112). Корпорации и акционеры, владеющие этими сетями, несомненно, выступают против таких рассуждений. Точно также, будут ли законной военной целью больницы, деятельность которых полностью зависит от этих сетей; они, скорее всего, будут рассматривать такие атаки, как атаки против защищаемых целей.

Если законы LOAC позволяют использовать нерегулярные силы, могут ли правительства нанимать хозяев ботов и использовать их ботнеты в качестве законных бойцов в киберконфликтах? Нерегулярные силы могут получить разрешение на участие в военных действиях, но ботнеты невозможно определить и их вооружение не видно.

Конечно, боты в ботнете не имеет эмблем или знаков отличия. Они могут даже не отслеживаться в отдельных ботах, потому что они распространяют вредоносные программы через веб-страницы, по одноранговым сетям, используя вредоносные ссылки, сайты социальных сетей и спам. Персональный компьютер, действующий в качестве бота в атаке, начатой по приказу государства, может принадлежать ни в чем не повинному гражданину, который не знает, что его компьютер был взломан. В случае поимки владельцев таких ботов, можно ли судить как военных преступников? А владельцев компьютеров?

В Гаагских конвенциях V и XIII изложены права и обязанности нейтральных стран в отношении войны на суше и на море, но они ничего не говорят о киберпространстве. Страна может не перемещать войск или конвоев по территории нейтрального государства или не совершать никаких враждебных действий в территориальных водах нейтральной стране, но что, если речь идет о прохождении сигналов по сетям нейтральных стран? Требуется ли странам получить разрешение нейтральных стран, для того чтобы осуществить кибератаки с использованием их сетей? Если используется технология коммутации пакетов, то каким образом страны вообще узнают о том, какие сети будут использоваться? Может ли страна использовать ботнеты в качестве нерегулярных сил, если в их составе действуют компьютеры, находящиеся в нейтральной стране?

Ни Хартия ООН, ни Женевская или Гаагская конвенции, ни Договор НАТО не говорят ничего о киберконфликте. И в Хартии ООН, и в Договоре НАТО используются такие термины, как "территориальная целостность", "применение вооруженной силы", "действия воздушными, наземными или морскими силами" и "вооруженное нападение", которые не вписываются киберсценарии, и, казалось бы, ставят их вне законов международного права. Конфликты в Эстонии и Грузии красочно иллюстрируют последствия киберконфликта, и путаница в отношении принятия мер реагирования обусловлена неопределенность в отношении законодательных правил[[113]](#footnote-113).

Аргументы в пользу геокиберстабильности

Выше обсуждены только несколько правовых неопределенностей в отношении киберконфликта. Обзор законов LOAC показывает наличие исторический готовности к обновлению этих документов, с тем чтобы они учитывали новые технологии, как это было сделано для военно-морского вооружения и воздушных судов[[114]](#footnote-114). Значит, в эти инструменты могут быть внесены дополнения, учитывающие киберконфликт.

Однако первым важным вопросом, является вопрос о том, какую степень активности следует считать допустимой? Автор утверждает, что в условиях киберконфликт должны применяться четыре принципа:

1Определенный объем критической инфраструктуры должен быть защищен для предотвращения ненужного разрушения, вреда и страданий и обеспечения минимально необходимой связи.

Защищаемая критическая инфраструктура будет включать такие, которые поддерживают, например, больницы и медицинские учреждения, центры для людей требующих опеки, финансовые системы, системы жизнеобеспечения и важнейшее медицинское оборудование, цепочки поставок, транспорта, новостные службы, образовательные учреждения, храмы и религиозные центры, службы экстренного реагирования и правоохранительные органы. Вышеприведенный перечень не является исчерпывающим, а лишь предлагает примеры типов систем, которые поддерживают жизнь мирного населения, в том числе детей, больных и раненых, а также пожилых. Вклад заинтересованных сторон должен помочь дипломатам определить священные границы критической инфраструктуры

Обоснование: Существующие законы LOAC поддерживает эту концепцию. Как отмечено в *Основных правилах Женевской конвенции и Дополнительных протоколах*:

В любом конфликте, право конфликтующих сторон выбирать методы или средства ведения войны не является неограниченным. Из этого принципа вытекают два основных правила. Первое запрещает применение оружия, снарядов, веществ и методов ведения военных действий, способных привести к ненужным травмам. Второе, в целях обеспечения уважения и защиты гражданского населения и гражданских объектов, обязывает Стороны конфликта постоянно делать различие между гражданским населением и бойцами, а также между гражданскими объектами и военными целями и направлять свои действия только против военных целей[[115]](#footnote-115).

Вред и ущерб, которые будут нанесены в результате уничтожения или недееспособности систем важнейшей инфраструктуры являются ненужными и могут привести к крайней степени страданий и тяготам такого характера, появления которого в соответствии с законами вооруженного конфликта требовалось предотвратить. Кроме того, поскольку эти сети обслуживают большую численность населения, вред и ущерб от такой атаки будет широкомасштабным и не пропорциональным полученным военным преимуществам.

Многие положения IV Женевской Конвенции в принципе поддерживают это предложение. Конвенция непосредственно касается защиты гражданских лиц и, в частности защищает раненых, больных, инвалидов, беременных женщин (Статья 16). Во время военных действий любая сторона может предложить нейтральные зоны в области конфликтов для защиты больных и раненых бойцов и мирного населения, а также гражданских лиц, проживающих в области конфликта, но участвующих в военных действиях и не выполняющих работ военного характера (Статья 15). Гражданские больницы, которые оказывают помощь раненым, больным, немощным и роженицам, ни при каких обстоятельствах быть объектом нападения (Статья 18). Детям в возрасте до 15 лет, являющимся сиротами или разлученным со своими родителями, должно быть обеспечено содержание, религиозные отправления и помощь в получении образования (Статья 24). Запрещается уничтожение любого движимого или недвижимого имущества, являющегося личной или коллективной собственностью частных лиц, страны или государственных органов, либо общественных или кооперативных организаций (Статья 53).

Протокол I Женевской конвенции дополняет Конвенцию IV и расширяет защиту гражданского населения во время войны. Особенно актуальны Статьи 4859 Протокола I. Гражданским лицом является любой человек, не являющийся членом вооруженных сил. (Статья 50). Гражданские лица пользуются общей защитой от опасностей, связанных с военными операциями, они не должны быть объектом нападения, подвергаться действиям, направленным на распространение террора или нападениям неизбирательного характера, которые не направлены на конкретные военные объекты, то есть атакам неизбирательного характера, которые, как ожидается, приведут к случайным потерям и ранениям гражданского населения, или к повреждениям гражданских объектов, которые чрезмерны по сравнению с военными объектами (Статья 51). Гражданские объекты не должны являться объектом нападения или ответных действий; в сомнительном случае объект считается гражданским (Статья 52). Враждебные действия не должны совершаться в отношении исторических памятников, произведений искусства или мест культовых отправления (Статья 53). Запрещены нападения на объекты, необходимые для выживания гражданского населения, таких как продукты питания, сельскохозяйственные районы, посевы, скот, установки обеспечения питьевой водой, а также ирригационные сооружения (Статья 54). Не должны подвергаться нападениям установки и сооружения, содержащие опасные элементы, такие, как плотины, дамбы и ядерные объекты, даже если они являются законными военными целями, если нападение на них могло бы привести к высвобождению "опасных сил и последующие тяжелые потери среди гражданского населения" (Статья 56). Должна проявляться постоянная осторожность в том, чтобы щадить гражданское население (Статья 57). Теми, кто планирует нападение, должны быть приняты все меры предосторожности, с тем чтобы объектами нападения не стали гражданские лица или гражданские объекты, находящиеся под особой защитой, и должны приниматься все возможные меры предосторожности, для того чтобы избежать и свести к минимуму случайные потери среди гражданского населения (Статья а 57). Запрещается нападать на неохраняемые территории, где не проводится военных операций и нет военного персонала (Статья 59).

Кроме того, законы LOAC содержат множество положений, которые были добавлены в последние годы и которые запрещают применение технологий, наносящих чрезмерные повреждения или имеют неизбирательное действие. Еще в 1899 году в дополнение к Гаагской конвенции были приняты Декларации, запрещающие запуск снарядов и взрывчатых веществ с воздушных шаров, "или другими новыми методами аналогичного характера"[[116]](#footnote-116), использование снарядов, распространяющих удушающие или вредные газы[[117]](#footnote-117), и применение пуль с расширяющимся или уплощающимся наконечником[[118]](#footnote-118). В 2001 году было принято Соглашение о запрещении или ограничении применения обычных вооружений, которые могут считаться наносящими чрезмерные повреждения, или имеющими неизбирательное действие, которая запретила широкий круг особо опасных и вредных вооружений, в том числе и указанное выше, начало использования которого датируется 1899 годом, а также противопехотных мин, мин-ловушек, зажигательного оружия, ослепляющего лазерного оружия и взрывоопасных следов войны[[119]](#footnote-119).. Это соглашение может быть дополнено, с тем чтобы учитывать кибератаки против определенных важнейших инфраструктур.

2 *Использование ботнетов и других нерегулярных киберсил должно быть объявлено вне закона.*

Обоснование: С точки зрения жертвы, в начале атаки, эти бойцы ничем не отличаются от любого другого нападающего; жертва не знает, является ли человек, атакующий систему, инсайдером, отдельным хакером или мошенником, высокоорганизованной преступной и террористической группой, или государством. Обнаружить и отследить деятельность злоумышленника в сфере киберпреступлений трудно, а иногда его подлинность не могут определить даже опытные следователи и исследователи, работающих по этому делу. Кроме того, киберсолдата третьей стороны невозможно отличить, потому что бойцы не могут носить отличительных знаков, и, безусловно, на расстоянии они ничем не отличаются. Таким образом, нерегулярные киберсилы нарушают одно из основных правил вооруженного конфликта.

3 *Страны должны уважать нейтралитет других стран и не должен передавать любые атаки через свои критические инфраструктуры (Гаагская конвенция V и XIII).*

Это согласуется с ограничениями Гаагской конвенции относительно перевозки войск или составов, расходных материалов и боеприпасов через нейтральные территории или воды. Многие важнейшие инфраструктуры, такие как электрические сети, в результате перегрузки системы могут быть уничтожены. Таким образом, позволяет странам проводить кибератаки, сигналы которых могли бы следовать транзитом через сети многих других стран без ведома последних, просто несовместимо с историей и намерениями законов LOAC. Предлагаемый принцип потребует, чтобы страны получали разрешения других стран, прежде чем начинать кибератаки, тем самым это требование также работает и как сдерживающий фактор против киберконфликта.

4 *Страны должны помогать друг другу в расследованиях киберпреступных действий.*

Решающее значение для обеспечения некоторой меры геокиберстабильности имеет сотрудничество с поставщиками интернета (ISP) и другими правительствами в расследовании злонамеренных действий. Несмотря на то, что даже во время войны требовать от нейтральной страны оказания помощи в расследовании, может показаться противоречащим правилам, все кибератаки выглядят одинаково в момент их начала. Только в ходе расследования жертва может получить представление о том, кто моет быть злоумышленником. В качестве основного принципа, страны, которые хотят быть подключены к интернету, должна быть обязаны гарантировать, что они и поставщики на их территории оказывают содействие в расследовании киберпреступлений. Если бы страны имели возможность отказаться от такой помощи под прикрытием нейтралитета, все киберпреступники получили бы отличный шанс для грабежа стран, участвующие в военных действиях. В обратном смысле, отказываясь помочь, нейтральные страны могут фактически оказаться пособниками и подстрекателями либо для преступников, либо для атакующей страны. В сценариях кибератаки страна может оставаться по-настоящему нейтральной то только путем оказания помощи.

Реализуя геокиберстабильность

Интернет создал киберпланету, которая не признает традиционных границ и действует в основном без контроля со стороны правительств. Он представляет собой новую форму оружия, которое создает беспрецедентный риск для гражданских лиц, особенно для детей и подростков, стариков, больных, хрупких или инвалидов. Он также переворачивает с ног на голову законы вооруженного конфликта, потому что, цели в киберконфликте, скорее всего, будут гражданскими, а не военными и он будет влиять на гражданское население, а не на войска. В большинстве стран важнейшая инфраструктура принадлежит частному сектору и управляется им. Следовательно, атаки на важнейшую инфраструктуру будет соответствовать нападению на гражданское население и именно на те самые сети, которые поддерживают их жизнь и дают и средства к существованию. Настоятельная необходимость обновить законы вооруженного конфликта для учета этой новой угрозы не может быть проигнорирована, потому что *отсутствие* правовой базы слишком легко интерпретировать как юридическое разрешение атаки.

Некоторые эксперты в области права и безопасности требуют создания большого закона или договора по киберпространству. Это нонсенс. За все время развития военно-морского флота, воздушного флота и других технологий, законы LOAC приспособились и остаются последовательной, но развивающейся, совокупностью правовых норм. Кроме того, есть и прагматические соображения. Договоры являются проблематичными, они требуют длительного, многостороннего обсуждения в фазе разработке, за которой следует открытие для подписания. Подписавшие затем должны ратифицировать договор и преобразовать его в национальный закон. Обычно чем договор вступит в силу, его должно ратифицировать определенное число стран, подписавших договор, и даже тогда, он действует только для тех стран, которые ратифицировали и внедрили его. Все это требует много времени, что играет на руку жуликам и злоумышленникам.

Однако во всех существующих документах, таких, как Хартия ООН, Договор НАТО, Женевская конвенция и Гаагская конвенция предусмотрена возможность внесения поправок, и их преимущество в том, что они уже ратифицированы и реализованы в национальных законах.

В киберпространстве, где важна каждая минута, очевидным решением является то, которое является наиболее целесообразным. Государства должны объединиться с заинтересованными сторонами, для того чтобы внести в существующие международные законы о вооруженных конфликтах следующие поправки:

1 В Хартию ООН следует внести поправки, учитывающие киберконфликт и уточняющие, что "территориальная целостность" включает в себя важнейшие инфраструктуры, а также кибердоступность, целостность и конфиденциальность. В частности, в Статью 42 следует внести дополнение, позволяющая Совету Безопасности действовать посредством киберсредств.

2 Договор НАТО, предусматривающие коллективную оборону в соответствии со Статьей 5. Термин "вооруженное нападение" в Статье 6(1) должен быть расширен в том, что касается "территории", а также "сил, судов и самолетов", с тем чтобы он охватывал кибератаки.

3 В Гаагскую конвенцию должны быть внесены дополнения, запрещающие использование нерегулярных сил в кибербоях и передачу сигналов кибератаки по сетям нейтральных стран.

4 В Женевскую конвенцию должны быть внесены дополнения, запрещающие атаки на ключевые инфраструктуры, которые наносили бы ущерб минимально необходимым коммуникациям и представляли и угрозу для гражданского населения.

Но если одна область, в которой требуется новое соглашение. Отдельно государства должна согласиться сотрудничать и оказывать помощь в расследовании деятельности злоумышленников, которые, как предполагается, осуществлялась по сетям данных государств. Страны, которые не подпишут такое соглашение, не должны иметь законной защиты в том случае, если международная связь из этой страны будет заблокирована другими странами.

Вышеизложенное позволит государствам и гражданам доверять информационно-коммуникационным технологиям и продолжать интегрировать их в свою жизнь и общество без страха за то, что они станут целями в киберконфликте. Такое положение дел также позволит начать конструктивный диалог между странами, в котором они впервые сядут за стол переговоров с общей позицией.

# 6 Кибермир

## Концепция кибермира

**Хеннинг Вегенер (Henning Wegener)**

Эта книга посвящена кибермиру, в отличие от преднамеренно отрицательных явлений кибервойны, кибертерроризма и киберпреступности. В антиномии войны-мира выбор, сделанный в пользу положительной стороны, предполагает важные изменения в перспективе и масштабе приоритетов, так как он концентрирует внимание на преимуществах и положительных возможностях информационного общества и ставит целью именно это явление, усиливая негативный оттенок кибервойны и связанных с ней ситуаций и бедствий, стимулируя динамичное движение в направлении глобальной культуры кибербезопасности

Эта попытка лишить кибервойну легитимности за счет обращения перспективы делается в полном сознании того, что цифровые инфраструктуры сегодня являются всепроникающими, и неизбежно будут использоваться также и во враждебных, а не мирных целях. Таким образом, главная цель заключается в том, чтобы воспрепятствовать такому использованию и максимально возможные строгие ограничения для любого применения ИКТ для враждебных действий. Поскольку сам термин "кибервойна" способствует стимуляции шаблона военного мышления, и термин киберзащита появился преимущественно в условиях военных действий и методов "возмездия", в этой главе будет сделана попытка борьбы с этим ментальным автоматизмом и попытка обосновать призыв к мирному поведение в киберпространстве. Тем не менее, она может не более, чем описать концептуальные основы кибермира, которые с течением времени должны быть конкретизированы. Многие другие разделы этой книги уже вносят свой вклад в решение этой определений задачи.

Уже в течение ряда лет, в том числе на открытых собраниях и в открытых публикациях Всемирная федерация ученых рассказывает о концепции кибермира, как о центральной теме своей работы[[120]](#footnote-120), и в последнее время МСЭ, в частности через своего Генерального секретаря, способствует тому, чтобы эта концепция стала более конкретной[[121]](#footnote-121), но этот термин, очевидно, использовался ранее, хотя и не в этом же всеохватывающем смысле. Наиболее заметное использование этого термина, хотя оно было очень специальным и ограниченным и касалось только детей, относится к 2007 году, когда он использовался Египтом в ходе содействия инициативной программы Кибермира в рамках Международного женского мирного движения Сюзанны Мубарак (Suzanne Mubarak) (SMWIPM)[[122]](#footnote-122), с прямой ссылкой на Декларацию и Программу действий ООН по культуре мира. Миссией этой инициативы является расширение прав и возможностей молодежи любой нации, за счет использования потенциала ИКТ, в направлении безопасности интернета и поощрения инноваций. Термин "кибермир" также иногда встречается, но бессистемно и неопределенно, в деятельности сообщества по исследованию проблем мира.

В данном контексте, кибермир, понимаемый намного шире, чем по версии SMWIPM, предназначен служить основным принципом в создании "универсального порядка в киберпространстве". Если использование термина относится больше к политике и имеет политический акцент, с ориентацией на правильный выбор, то отсюда следует также, что он должна оставаться несколько открытым. Определению не может быть неоспоримым но оно должно быть интуитивно понятным, а также допускать дополнения списка ингредиентов

Тем не менее, требуется основное определение. Отправной точкой для любой такой попытки дать определение должна быть общие концепция мира как благоразумного состояния покоя, отсутствия беспорядков или нарушений и насилия, отсутствия не только "прямого" насилия либо применения силы, но и косвенные ограничений. Мир подразумевает распространение правовых и общих моральных принципов, возможностей и процедур для урегулирования конфликта, долговечности и стабильности.

Всеобъемлющей попыткой сформулировать концепцию мира и культуры мира со значимым содержанием мы обязаны Генеральной Ассамблее ООН. Ее "Декларация и Программа действий по культуре мира" от октября 1999 года[[123]](#footnote-123) содержит каталог ингредиентов и предпосылок мира, а также очерчивает путь достижения и поддержания его с помощью культуры мира. Ссылаясь на Хартию Организация Объединенных Наций по вопросам образования, науки и культуры, которая гласит, что "войны начинаются в умах людей, поэтому защита мира должна быть построена в сознании люде", Резолюция подробнейшим образом описывает элементы, а ставит точки действия на десятилетие до 2010 года.

Важными элементами мира и культуры мира являются не только неприменение силы и продвижение практики ненасилия, но и общий набор ценностей и моделей поведения, международный порядок и законность, позитивные, динамичные процессы участия и права человека (в частности, упоминается, соблюдение принципов свободы, справедливости, демократии, толерантности, солидарности, сотрудничества, плюрализма, культурного разнообразия, диалога и взаимопонимания, содействие в урегулировании конфликтов). Помимо наиболее явно акцентируемых этических компонентов мира, в контексте киберситуации особенно важно, чтобы этот список включал в себя в числе предпосылок мира уважение и поощрение права каждого на свободу выражения мнений, убеждений и информации, а также на доступ к информации. Эти указания, конечно, носят всего лишь ориентировочный характер; резолюция в целом предполагает внимательное прочтение. Не так давно МСЭ сформулировал пять принципов, кибермира, которые также устанавливают конкретные действия и обязательства, которые будут обеспечивать мир и стабильность в киберпространстве. Читатель может обратиться к этому списку, так как он имеет конструктивное значение.

Всемирная федерация ученых со своей стороны взяла на себя обязательство перевести общие принципы, содержащиеся в нем, а также другие общие утвержденные ООН принципы, применимые к киберсреде более подробно в своей " Декларации Эриче о принципах киберстабильности и кибермира", август 2009 года[[124]](#footnote-124).. Эта Декларация показывает, что достижение киберстабильности и кибермира тесно взаимосвязаны. Декларация является краткой и концентрируется на основных рабочих моментах кибермира. К ним относятся следующие:

1 Все правительства должны признать, что международный закон гарантирует лицам свободный поток информации и идей; эти гарантии также распространяются на киберпространство. Ограничения должны налагаться только по мере необходимости и их должен поддерживать процесс для правового пересмотра.

2 Все страны должны совместно разработать общий кодекс киберповедения и глобально гармонизированные правовые рамки, включая процедурные положения, касающиеся помощи в проведении расследований и сотрудничества, которые уважают неприкосновенность частной жизни и прав человека. Все правительства, поставщики услуг и пользователи должны поддерживать международная правоохранительные действия, направленные против киберпреступников.

3 Все пользователи, поставщики услуг и правительства должны добиваться того, чтобы киберпространство не использовалось каким-либо образом, который приводил бы к эксплуатации пользователей, особенно молодых и беззащитных, посредством насилия или деградации.

4 Правительства, организации и частный сектор, в том числе физические лица, должны внедрять и поддерживать комплексные программы безопасности, основанные на международно признанном передовом опыте и стандартах с использованием технологий конфиденциальности и безопасности.

5 Разработчикам программного и аппаратного обеспечения следует стремиться к разработке безопасных технологий, которые способствуют устойчивости и противостоят уязвимости.

6 Правительства должны активно участвовать в усилиях Организация Объединенных Наций по поощрению глобальной кибербезопасности и кибермира, с тем чтобы воспрепятствовать использованию киберпространств для конфликта.

За этими принципами, и особенно за номером шесть, признается твердое намерение использовать конфликтный потенциал в киберпространстве. И действительно, в свете тревожного роста наступательных возможностей "кибервойны", особое внимание в поисках кибермира, должно уделяться воинственным аспектам деятельности в киберпространстве, как со стороны правительства, так и со стороны неправительственных нарушителей.

Эти проблемы подробно рассмотрены в других частях этой книги. Тем не менее, несколько заявлений о принципах соответствуют настоящему контексту выяснения, что такое кибермир. Киберпространство пока, в слишком большой мере, является пространством, свободным от законов, открытым для всех бесплатно, без указаний или санкций, и, казалось бы, дающим разрешение на юридически неограниченного действия. Поэтому и появился призыв к созданию общих кодексов киберповедения во всех цифровых сферах. Всемирная федерация ученых, начиная с 2001 года, призывает к работам над всеобщим Законом о киберпространстве, желательно под эгидой Организации Объединенных Наций[[125]](#footnote-125). Такой закон нигде не является более уместным, чем в области наступательного военного использования киберпространства.

Сложность этой задачи, а также правовые и – возможно, прежде всего – политические препятствия на этом пути очевидны. Как отмечается в других местах в этой книги, традиционные законы войны и вооруженных конфликтов являются неоднозначными или их польза очень ограничена, а определения отсутствуют. Ссылки на традиционные пределы действий, указанные в основных текстах международная закон, таких как Хартия ООН или Договор НАТО, в значительной степени бесполезны. Текст Женевской конвенции и некоторых резолюций и конвенций Генеральной Ассамблеи ООН, например, в области

транснациональной организованной преступности, терроризма или поведения в космическом пространстве, дают, в лучшем случае, разрозненные и неполные аналогии[[126]](#footnote-126). "Контроль вооружений" или разграничение между законным и "незаконным" использованием ИКТ, или между преступлением и обороной, являются туманными, так как технологии являются идентичными, и проблема "двойного назначения", которая окружает контроль над вооружениями, в очень многих аспектах присуща и этой ситуации. Кроме того, дилемма отыскания и отслеживания  присвоение авторства, надежные и подходящие сроки, которая уже делает проблематичным преследование "простой" киберпреступности, в военной области умножается на вероятность того, что воинственный злоумышленник будет использовать максимально сложные методы уклонение от ответственности и маскировки. Проверка, важный элемент контроля вооружений, здесь практически невозможна. Сдерживание в его традиционном смысле не является жизнеспособным, когда его отсутствуют основные характеристики (установление авторства, место происхождения, уровень ответственности). Поэтому логично, что авторитетные публикации утверждают, что наиболее подходящим вариантом является ставка на киберзащиту, в том числе на "расширенную" с помощью союзников киберзащиту, а не на киберсдерживание само по себе[[127]](#footnote-127).

Тем не менее, если принять концепцию кибермира всерьез, правовая основа имеет большое значение для определения того, что представляет собой нарушение мира, и государства не должны оказаться под гипнозом недостатков, присущих таким рамкам. В своей концепции Генеральный секретарь МСЭ, пошел дальше пяти принципов МСЭ, и предположил, что страны в таком документе должны взять на себя обязательства не наносить первыми киберудар против другой страны ("неприменение первыми"), и должны взять на себя обязательства не оставлять в своей стране безнаказанными кибертеррористов и нападающих[[128]](#footnote-128). Страны можно также поощрять к заключению двусторонних или многосторонних пактов о не применении киберагрессии. В них могут содержаться взаимные обязательства о ненападении на важнейшие инфраструктуры страны, особенно те, которые имеют гуманитарные цели или служат основным потребностям человека, которые уже частично защищены существующими международными законами, и может подтвердить неприкосновенность трансграничных сетей передачи данных. Важным и смелым шагом для международного инструмента было бы лишение легитимности наступательных кибервооружений и наступательных стратегий для их использования

В действительности, такие стратегии и принципы, предназначенные для содействия кибермиру, по всей видимости, не могут рассчитывать на мгновенную поддержку многих стран, которые уже серьезно вложились и продолжают инвестировать в потенциал кибервойны, извлекая для себя пользу из в нынешнего правового вакуума в киберпространстве. Действительно, последние отчеты о систематическом "вооружении" киберпространства, создание киберкоманд, разработки наступательных киберстратегий и т. д. отнюдь не обнадеживает. Тем не менее, не следует недооценивать моральные последствия многосторонних мер противодействия. Законность является важным инструментом государственного управления, и сам факт того, что определяются границы для действий, формируются и согласовываются критерии, со временем может создать и импульс, и мотивацию. Кибермир, для того чтобы внести свой вклад в киберстабильности и основные права, требует определенных действий для его обеспечения.

Для этой цели существует мощное обоснование. Функционирование и стабильность взаимозависимой глобальной сетевой структуры и доверие к ней является всеобщим общественным благом. Массовые кибератаки даже, если они совершаются только в одном сегменте системы, трудно контролировать; их последствия могут быть неисчислимыми, Даже незначительным событиям свойственна тенденция неуправляемой цепной реакции[[129]](#footnote-129). Они могли бы решительно изменить мощные уравнения, геостабильность всей цифровой среды, от которой зависит общество, выходит далеко за пределы возможностей сторон в конфликте. Интерес в поддержании транснациональных сетей и информационных структур является интересом, который разделяют все участники международных процессов.

Не требуется доказательств тому, что неспровоцированные наступательные кибердействия, и тем более любая кибератака несовместимы.

Но концепция проходит свое решающее испытание, когда дело доходит до определения и оценки *реакции* на ожидаемые или реальные кибератаки, в том случае, когда имеет место киберконфликт. Если – или когда – кибератака является или не является вооруженным нападением: есть общее соглашение относительно того, что преимущество здесь получает главный принцип международного закона о праве на самооборону *в самом общем смысле* правомерности защиты себя и предотвращая нападения. Как уже неоднократно отмечалось в этой книге, определение враждебных действий, как "вооруженного нападения" является, с точки зрения Хартии ООН, Договора НАТО и общего международного права, является необходимым для запуска механизмов законной индивидуальной и коллективной защиты *военными средствами*. Конечно, говорить о том, что кибератака на другое государство или с последствиями в другом государстве является таким "вооруженное нападением" или его эквивалентом, можно тогда, когда она, по крайней мере, влечет серьезные разрушения или людские потери[[130]](#footnote-130).

Тогда это могло бы обеспечить правовую основу для коллективных действий, в том числе военными средствами. Но определение и возможность ответных военных действий в контексте цифровых технологий требует нового тщательного размышления и, в конечном счете, политики преднамеренного сдерживания.

Различия между киберконфликтом и традиционной физической "войной" являются яркими и выходят за рамки очевидной разницы в используемом "вооружении". Резюмируя аргументы, предложенные во многих других разделах этой книги, в том числе в этой главе, в первую очередь, следует вспомнить о неопределенности в определениях и уровнях определения кибератак, в результате чего становится неопределенным адресат любых контрмер или возмездия, против кого они могут быть законно направлены? Тогда, благодаря всепроникаемости и взаимосвязанности цифровых сетей и систем, последствия цифровых контрмер непредсказуемы и, следовательно, трудно масштабировать эскалацию воздействия любых контрмер. В-третьих, киберконфликт может перерасти в большую скоординированную и, следовательно, деструктивную атаку, или он может принимать вид повсеместного состояния вечной угрозы низкого уровня (кибершпионаж, создание неизвестных ботнетов, и т. д.) с различной степенью возможности перерастания в далеко идущие разрушения инфраструктуры. В контексте межгосударственного конфликта, есть и новизна наличия бесконечного числа возможных участников; уроки "холодной войны" второй половины прошлого века, поддержание военно-ядерного баланса двух держав с уникальным сочетанием сдерживания и сдержанности, не могут быть просто перенесены на враждебные сценарии с несколькими участниками. Наконец, как уже было подчеркнуто, все заинтересованы в сохранении функционирования мировой информационной инфраструктуры.

Эти различия, и другие, которые можно было бы привести, должны сформировать наше мышление относительно реакции на нападение. В соответствии с концепцией кибермира, приоритет должен быть отдан поддержанию или скорейшему восстановлению мирной и стабильной обстановки. Это делает четкий акцент на оборону.

Превентивная самооборона является ключом к реакции, совместимой с миром. Согласно этой концепции, в цифровой среде должна быть признана общая ответственность всех заинтересованных сторон в обеспечении себя безопасными сетями и системами, и это требование также имеется в Декларации Эриче. Сотрудничество межу компаниями и правительством также важно, как международная сотрудничества. Ключевым условием является устойчивость: не только качество систем, но и управление ими должны вносить вклад в надежность и непроницаемость для атаки. Заинтересованные стороны должны оптимизировать свою осведомленность о ситуации на своих сетях, выявляя ценные активы и уделяя внимание их уязвимости (контроль всей сети в реальном времени, внедрение зон безопасности, сегментация сети, обеспечения энергетической безопасности). Следовательно, жизнеспособные системы и программное обеспечение, строгое соблюдение протоколов и стандартов МСЭ и национальной безопасности, должны получить широкое распространение. Устойчивые ИТ-инфраструктуры препятствуют атакам и вносят вклад в создание мирной обстановки. Отличная оборона является одним из важнейших элементов киберстабильности; превосходная защита сдерживает нападения, так как она вносят вклад в повышение доверия, и позволяет операторам чувствовать себя комфортно

Устойчивость, как она обычно определяется, включает в себя несколько элементов, среди которых самовосстановление качества систем, наличие систем оповещения, встроенная избыточность, а также отработанные режимы поведения, такие как изучение областей сотрудничества в рамках сообщества заинтересованных сторон как части мирной обстановки, расширенный обмен информацией, короче говоря, упор делается на позитивные действия и поощрения на практике. Государства, интересующиеся вопросами киберконфликтов, и, желающие участвовать в противодействии возможным сценариям киберконфликт, также могут рассмотреть варианты нормативной деятельности на высоком уровне, такие как понимание некиберагрессии, механизмы обеспечения прозрачности с целью разрушения образов врага, мониторинг недоброжелательности и обмен информацией, позволяющий лучше определить виновных в случае конфликта. Некоторые из этих предложений также включены в ранее цитируемое предложение Генерального секретаря МСЭ. Зарождающийся глобальный механизм раннего предупреждения (Глобальный центр реагирования (GRC), Сеть раннего предупреждения (NEWS) или ESCAPE) имеют очевидное значение в аспекте применения ненасильственных мер. Рамки международного сотрудничества должны использовать все более обширные сети CERT.

Тем не менее, должны быть составлены положения для сценариев серьезных киберконфликтов, в которых просто пассивные оборонительные действия недостаточны, и в соответствии с международным законом право должен быть прописано на активную самооборону. С точки зрения кибермира, здесь опять-таки были бы неуместными простые аналогии с традиционным правом вооруженных конфликтов. Они содержат риски того, что ментальная концепция, созданная таким образом, приводит к ответным сценариям военных действий и военной логике максимального уничтожения вражеских активов. Обращение к традиционным Правилам ведения боевых действий может привести к опасным результатам. Кибермир не требует полного отказа от противодействия наступлению и мести, но нюансы в значительной степени меняют применимые сценарии.

Здесь в разработке ответных мер ключевым термином будет *сдержанность*. Ее элементы будут включать строгий и постоянный анализ угроз и рисков для предотвращения неконтролируемых последствий, в том что касается выведения из строя всеобъемлющей киберсети; концентрацию на хорошо подобранных ответных мерах без эскалации; терпение и своевременность ответа, с тем чтобы обеспечить лучшее определение атаки, активировать резервы и одноранговые оборонительные союзы; тщательность в применении принципов необходимости и соразмерности, присущих разрешенной самообороне; и тщательная защита важнейшей инфраструктуры гуманитарного или социально необходимого характера.

Хотя, возможно, будет преувеличением утверждать, что в ответах на кибератаки оборона *всегда* является лучшим наступлением, кибермир, в настоящем анализе, по всей видимости, не требует, наряду со строгими ограничениями мести, принципа всеобъемлющего приоритета самообороны перед наступлением[[131]](#footnote-131). Как отмечалось выше, этот принцип будет соответствовать призыву к систематической делегитимации на государственном уровне кибер "оружия" и наступательных киберстратегий.

# 7 Международный ответ кибервойне

**Хамадун И. Туре (Hamadoun I. Touré)**

## 7.1 Национальная политика и подходы

Страны во всем мире реагируют на новые угрозы кибервойны различными способами. Хотя некоторые государства еще только начинают рассматривать вопрос о кибербезопасности[[132]](#footnote-132), большинство правительств, как минимум, признают необходимость перераспределения ресурсов и реформы национальных стратегий безопасности на некотором уровне. Многие страны увеличивают объем финансирования, исследований, а также тактических и дипломатически ресурсов для улучшения кибербезопасности[[133]](#footnote-133). Некоторые страны принимают участие в "сокращении разрыва", стремясь изолировать определенные сети, не позволяя им связываться с другими системами с целью защиты от атак важнейшей информационной структуры и систем[[134]](#footnote-134). В следующем разделе дается оценка различных подходов, принятых различными государствами.

**a) Внедрение кибервозможностей в обычную стратегию военных действий**

Когда дело доходит до кибертактики, создания наступательных кибервооружений и оборонительных возможностей, некоторые страны изучают традиционный подход к ведению военных действий. Они рассматривают кибероружие, как "усилитель силы", который должен использоваться в основном в ходе традиционных военных действий в целях значительного повышения их боевого потенциала[[135]](#footnote-135). За последние годы интернет стал важным средством обмена информацией и пропаганды во время вооруженного конфликта. В этой связи многие страны рассматривают информационную диверсии в сети интернет как форму военной агрессии против общественной морали, и поэтому они готовы ответить на кибератаки с применением военной силы[[136]](#footnote-136). Недавние инциденты, повлекшие за собой утечку секретных военных документов, ясно показывают, почему государства беспокоятся о возможных последствиях киберуязвимости для морали и общественной поддержки[[137]](#footnote-137). Некоторые государственные чиновники указывают, что в прошлом они могли бы считать тактику информационной войны военными действиями, вне зависимости от того привела ли она к жертвам, и, следовательно, военный ответ был быть оправданным[[138]](#footnote-138).

**b) Разработка кибертактики как национального ресурса**

Благодаря перераспределению ресурсов и финансов, а также изменению стратегического планирования, многие страны рассматривают свою цифровую инфраструктуру и ИКТ как национальный ресурс или стратегический актив. Некоторые страны даже явно сформулировали это как новую национальную политику[[139]](#footnote-139). Страны переводят бюджетные ресурсы на финансирование инициатив в киберпространстве, выделяя значительные суммы для исследований и разработки средств для кибервойны[[140]](#footnote-140). Некоторые правительства сформулировали и начали выработку единых национальных планов, учитывающих новые киберугрозы, мобилизуя различные сектора и полностью преобразовав ресурсы и стратегию[[141]](#footnote-141). Этот вид преобразований может включать обучение или переподготовку военнослужащих, изменения в структуре спецслужб, которые должны сосредоточиться на сборе соответствующей научной и технической информации и осуществлении моделирования боевых действий и военных учений кибервойны, уделяя при этом особое внимание применению информационных технологий[[142]](#footnote-142). Ряд стран приступили к проведению национальных конкурсов для выявления и найма на работу сильнейших киберумов среди гражданского населения[[143]](#footnote-143). Они также стимулируют своих отечественных производителей к разработке более совершенных технологических возможностей в поддержку новой военной стратегии. Некоторые правительства также работают над созданием пула частных гражданских хакеров, которых можно было бы призвать в случае необходимости[[144]](#footnote-144). Эти "хактивисты" могут быть технически образованными специалистами или даже бывшими незаконными хакерами, которых наняли и обучили ,с тем чтобы использовать их навыки в целях национальной безопасности[[145]](#footnote-145). Некоторые страны могут даже использовать проксихакеров, т. е. наемных хакеров и специалистов из других стран, которые действуют от их имени[[146]](#footnote-146). Все эти изменения демонстрируют отход от реактивной стратегии в отношении киберугроз и переориентацию на разработку активной тактики ведения информационной войны для эффективных действий в условиях высоких технологий[[147]](#footnote-147).

**c) Создание военных киберсредств**

Некоторые страны отреагировали на новые угрозы кибервойны, выделяя для ведения виртуальных боев большое количество военного персонала[[148]](#footnote-148). Этот сдвиг в политике может предусматривать создание команд для войны в интернете, предназначенных для обеспечения кибербезопасности, которые могли бы быть интегрированы в другие спецслужбы[[149]](#footnote-149), или даже создание совершенно новых секторов военной структуры, предназначенных для кибердеятельности[[150]](#footnote-150). Эти новые военные средства, созданные, для того чтобы объединить и подготовить военные ресурсы для полномасштабных операций в киберпространстве[[151]](#footnote-151). Хотя зачастую их основная сфера деятельности состоит в защите военных сетей и проведении военных операций в киберпространстве, им также могут быть поставлены задачи защиты частных сетей, которые также обеспечивают ведение многих военных операций[[152]](#footnote-152).

**d) Применение кибертактики, для того чтобы уравнять правила игры**

Совершенствуя тактики информационной и электронной войны, некоторые страны надеются уравнять правила игрысо странами, которые полагаются на то, что программное обеспечение и компьютерные системы усилят их обычные вооруженные силы. Этот переход включает в себя инвестиции в новые автоматизированные командные системы, в том числе такого оборудования как волоконно-оптические кабели, спутники и высокочастотные цифровые радиосистемы, а также повышенное внимание в отношении космических, воздушных, морских и наземных систем наблюдения[[153]](#footnote-153). Некоторые правительства уже используют ИКТ, управляемые технически грамотными военнослужащими, для мониторинга национальных границ[[154]](#footnote-154). Новые киберориентированные стратегии могут даже в большей степени полагаться на эти ресурсы, и сопутствующие им автоматизированные системы для охраны границ. Другие тактические действия могут включать в себя операции управления и контроля, которые направлены на разрушение информационных потоков противника и нацелены на вражеские инфраструктуры ИКТ, стремясь повредить и уничтожить важнейшее оборудование, сети и данные[[155]](#footnote-155). Эти изменения сосредоточены на атаке на слабые места потенциальных противников, а именно, на их зависимость от киберпространства и новых технологий. Страны, которые имеют сильные возможностей и для традиционных боевых действий, и для кибервойны, на самом деле могут оказаться наиболее уязвимыми, потому что их укрепляет технология, которая уязвима для новых видов атак, таких как логические бомбы и взлом[[156]](#footnote-156). Инвестируя в потенциально асимметричные действия в киберпространстве, страны надеются нейтрализовать военные возможности своих противников[[157]](#footnote-157).

**e) Обучение граждан и повышение осведомленности о кибербезопасности**

Многие правительства признают, что обучение и повышение осведомленности населения являются мощными методами киберзащиты[[158]](#footnote-158). Информационные базы данных и национальные месячники повышения осведомленности, проводимые правительством или частными организациями, помогают повысить информированность на низовом уровне[[159]](#footnote-159). Эти программы часто сосредотачиваются на обучении отдельных пользователей и небольших компаний тому, как защитить свою информацию и системы от таких киберпреступлений, как кража личных данных и взлом. В большинстве случаев незаконный доступ к компьютерной системе является лишь жизненно важным первым шагом, и взлом отдельных компьютеров или системы может стать предпосылкой для дальнейших преступлений, затрагивающих национальную безопасность, таких как информационный шпионаж или атаки типа "отказ в обслуживании". Когда такие "преступления" совершаются в отношении жизненно важных национальных ресурсов или правительственных органов, их более точно назвать кибератаками или кибервойной. Хакеры регулярно и с заметным успехом пытаются проникнуть в правительственные системы, системы частного бизнеса и национальные системы обороны[[160]](#footnote-160). Информационный шпионаж или доступ к конфиденциальной информации могут осуществляться как с использованием технических средств, так и методами "социальной инженерии", тактика которых опирается на взаимодействие с человеком с целью обманом заставить людей дать доступ к системам, которые в ином случае были бы защищенными[[161]](#footnote-161). Следовательно, осведомленность населения об использовании методов социальной инженерии и таких технических методов, как размещение в общественных местах зараженных флеш-накопителей, может содействовать защите национальных ресурсов[[162]](#footnote-162).

**f) Наименее соединенные и развивающиеся страны**

Хотя важнейшие инфраструктура и услуги во многих странах сильно зависят от ИКТ и интернета, другие группы населения не являются также зависимыми или соединенными, и используют не ИКТ в целом, а национальные внутренние сети или другие ресурсы. Однако даже эти страны, по всей видимости, увеличивают свои онлайновые возможности, хотя такие достижения могут быть ограничены военными и правительственными применениями[[163]](#footnote-163). Страны, которые переходят на он-лайн позже, могут столкнуться с меньшей уязвимости к кибератакам, так как их правительственные системы в целом имеют меньше связей с остальной частью киберпространства[[164]](#footnote-164). Но даже развивающиеся страны, которые еще не обладают инфраструктурой, для того чтобы в полной мере пользоваться всем спектром преимуществ, которые стали возможными благодаря ИКТ, все еще зависят от интернета и других мобильных и цифровых технологий, которые удовлетворяют ряд их основных потребностей[[165]](#footnote-165). Таким образом, они тоже заинтересованы в будущей кибербезопасности.

## 7.2 Недавние международные ответные действия

Сегодня на противодействие угрозе кибервойны направлено гораздо меньше международных усилий, чем имеется национальные стратегии, хотя некоторые попытки многосторонние инициативы уже делаются. Двусторонние подходы были также делаются, но они далеки от всеобъемлющей стратегии по улучшению кибербезопасности и обеспечению кибермира, так как в них вовлечена очень малая доля участников уравнения кибермира. Некоторые страны призывают к созданию договора по ограничению применения кибероружия, в то время как другие считают, что такой договор является либо ненужным, либо преждевременным[[166]](#footnote-166). Хотя эти предложения могут служить доказательствами движения к международному сотрудничеству, они далеки от по-настоящему комплексного подхода и четкой стратегии продвижения вперед, которые объединили бы все заинтересованные стороны. В следующем разделе представлены некоторые недавние международные ответные действия, хотя он и не содержит их исчерпывающего перечня.

**a) Управление ООН по наркотикам и преступности (UNODC) – Конгресс по предупреждению преступности и уголовному правосудию ООН (UNCPCJ)**

В апреле 2010 года двенадцатый Конгресс по предупреждению преступности и уголовному правосудию Организации Объединенных Наций (UNCPCJ) подготовил проект набора Деклараций, которые содержали положения, призывающие к созданию межправительственной группы экспертов для изучения проблемы киберпреступности и международного реагирования[[167]](#footnote-167). Соответственно, в ходе 19-й сессии Комиссии по предупреждению преступности и уголовному правосудию государства-члены сделали соответствующую рекомендацию, обратившись к комиссии с просьбой создать межправительственную группу экспертов открытого состава для выполнения положений Конгресса UNCPCJ[[168]](#footnote-168). Хотя Конгресс не пришел к консенсусу в вопросе подготовки нового договора по киберпреступности, это привело к подписанию соглашений о технической помощи и создании потенциала, которые уже являются хорошей основой для обсуждения дальнейших действий[[169]](#footnote-169).

**b) Экономический и социальный совет ООН (ECOSOC)**

Экономический и социальный совет ООН (ECOSOC) открыл свою сессию 2010 года с брифинга по проблемам кибербезопасности, а также угроз и возможностей, предоставляемых постоянно расширяющимся использованием интернета. Среди прочего, Совет подчеркнул необходимость международных инициатив, которые были бы направлены на обмен информацией и передовым опытом, подготовку кадров и научные исследования. Кроме того, эксперты заявили, что Организация Объединенных Наций должна действовать по этому вопросу "как единое целое", что должно усилить не только сотрудничество между странами, но и сотрудничество между государствами и частным сектором в целях обеспечения кибербезопасности[[170]](#footnote-170). Они предупредили, что международная область действия и катастрофические последствия реальной кибервойны требуют скоординированных ответных мер; а специальные решения и укрепление обороны в настоящее время являются недостаточными стратегиями[[171]](#footnote-171).

**b) Организация Североатлантического договора (НАТО)**

В 2008 году НАТО внедрил собственную политику киберзащиты в целях защиты своих технологических ресурсов и интересов стран членов[[172]](#footnote-172). В рамках этой политики альянс создал Административный орган управления киберзащиты, средства нанесения ответного удара в случае компьютерных инцидентов, которые предусматривает отправку команды быстрого усиления в отдельную страну-член, и Совместный Центр компетенции по киберзащите[[173]](#footnote-173). Расположенный в Эстонии, Центр объединяет экспертов, которые проводят исследования и подготовку кадров в области кибербезопасности. Его спонсорами являются Эстония, Латвия, Литва, Германия, Италия, Словакия и Испания[[174]](#footnote-174).

Кроме того, НАТО также провел учения по киберзащите, в которых команды от государств-членов стремились защитить виртуальные компьютерные сети от кибератак. Такие учения предназначены для более глубокого понимания международной киберсреды и расширения международного сотрудничества в противодействии инцидентам[[175]](#footnote-175). НАТО также подписал с Эстонией, США, Великобританией, Турцией и Словакией меморандумы о взаимопонимании, связанные с кибербезопасностью[[176]](#footnote-176).

**c) Совет Европы – Будапештская конвенция о киберпреступности**

Конвенция о киберпреступности Совета Европы[[177]](#footnote-177) касается определенных киберпреступлений, предоставляя типовые законодательные положения, которые страны могут принять и адаптировать к своим конкретным потребностям. Хотя Конвенция содержит некоторые правовые решения для таких преступлений, как незаконный доступ (взлом) и перехват, в ней не учтены некоторые наиболее опасные виды кибервторжений, например, информационный шпионаж и саботаж. И хотя Конвенция содействует укреплению международного сотрудничества путем установления уголовной ответственности за основные киберпреступления, ее предписывающая власть ограничена в результате стремления разработчиков проекта не нарушать другие национальные законы, которые могут с ним конфликтовать. При таком подходе значительные культурные и правовые различия замедляют создание единого закона, если не делают это совершенно невозможным[[178]](#footnote-178). Только тридцать стран ратифицировали этот договор с момента его открытия для подписания в ноябре 2001 года, и только одна из этих стран не входит в состав Европы[[179]](#footnote-179).

Правовые нормы, такие как изложенные в этой Конвенции, являются одним из способов противостояния некоторым угрозам национальной и международной кибербезопасности. Тем не менее, положения Конвенции не дают прямого решения проблемы кибервойны между странами. Хотя угроза санкций может удержать некоторых киберпреступников, законодательство такого рода не может идти достаточно далеко в сдерживании злоумышленников, которые уверены в том, они могут избежать раскрытия, идентификации и судебного преследования

**d) Двусторонние соглашения по кибербезопасности**

Отдельные государства также пытаются строить отношения с другими странами в сфере кибербезопасности. Например, руководство Министерства связи и информационных технологий Индии стремится к сотрудничеству в форме меморандумов о взаимопонимании или иного документа с различными странами и поддерживает обмен информацией. Например, в 2004 году Индия и Южная Корея подписали совместное заявление о двустороннем сотрудничестве в области информационных технологий (ИТ). Команда экстренного компьютерного реагирования Индии также подписала меморандум о взаимопонимании с Национальным Центром кибербезопасности Кореи с целью установления официального сотрудничества, среди прочего, в области кибербезопасности[[180]](#footnote-180). Индия также имеет ряд других двусторонних договоренностей, связанных с ИТ в целом и несколько с особым акцентом на кибербезопасность и киберпреступность[[181]](#footnote-181). Во время регионального конференции по кибербезопасности в Марокко в начале этого года Марокко и Малайзия также подписали меморандум взаимопонимании в области кибербезопасности[[182]](#footnote-182). Меморандум создал отношения сотрудничества между министерствами кибербезопасности двух стран, охватывая, в том числе защиту важнейших информационных инфраструктур, разработку программ кибербезопасности, создания потенциала, профессиональную подготовку и осведомленность. Хотя эти виды сотрудничества могут улучшить кибербезопасность страны, их одних недостаточно, для того чтобы защитить любую отдельно взятую страну от глобальной кибервойны. Следовательно, для обеспечения мира для всех народов требуется всеобъемлющая, глобальная структура, связанные с кибербезопасностью.

**e) Международный союз электросвязи (17-я Исследовательская комиссия МСЭ-T) – Глобальные стандарты**

Для решения вопроса о кибербезопасности в частности, в отношении умных электросетей, МСЭ создал оперативную группу по умным электросетям, которая будет собирать и документировать информацию и идеи, которые будут полезны для разработки рекомендаций в поддержку умных электросетей с точки зрения электросвязи[[183]](#footnote-183). Оперативные группы являются инструментом МСЭ, который дополняет программы работ Исследовательских комиссий агентства путем предоставления альтернативной рабочей среды для быстрой разработки спецификаций в определенной области[[184]](#footnote-184). Оперативные группы в настоящее время широко используются для решения проблем промышленности по мере их возникновения, что делает их идеальными для быстро меняющихся и развивающихся технологий, таких как умные электросети, Оперативная группа по "умным" электросетям (FG Smart) состоит из представителей различных государств-членов и будет сотрудничать с мировым сообществом в области умных электросетей, например, научно-исследовательскими институтами, форумами, научными кругами. Для достижения своей цели по разработке рекомендаций для стандартов "умных" электросетей, оперативная группа будет поддерживать обновляемый перечень органов по стандартизации, занимающихся умными электросетями, собирать идеи и ценные предложения для умных электросетей, обеспечить терминологию и таксономию, необходимые для поддержки умных электросетей, собирать новые идеи, соответствующие потенциальным областям исследований и выявляющие их для поддержки умных электросетей, а также определить потенциальные последствия разработки стандартов в таких проблемных областях, как безопасность, конфиденциальность и совместимость[[185]](#footnote-185). Все эти мероприятия обеспечат комплексный и многогранный подход к быстро развивающимся и растущим проблемам кибербезопасности, связанным с "умными" электросетями.

Кроме того, используя свои связи с Сектором стандартизации электросвязи МСЭ (МСЭ-Т), одной из самых признанных организаций по созданию стандартов электросвязи, оперативная группа сможет служить объединяющим и надежным источником информации и рекомендаций, имеющих репутацию качественных стандартов, основанных на консенсусе. Отношения с МСЭ-Т также создает благоприятные условия для проведения, при желании, результирующих документов оперативной группы через Исследовательскую комиссию в виде рекомендаций МСЭ-T, добавлений, руководств и т. д. В рамках МСЭ-Т, Оперативная группа сможет добиться большего признания своих спецификаций на многих мировых рынках, в частности в развивающихся странах и в других регионах, отличных от тех, которые активно участвуют в работе конкретного форума.

## 7.3 Необходимость международных рамок

**a) Нежизнеспособность сдерживания**

С появлением каждой новой области приходят новые проблемы. Так же, как театры военных действий на земле, на море, в воздухе и космическом пространстве ставили новые вопросы распределении и эффективного использования ресурсов в ходе разрешения прошлых и современных конфликтов, так и киберпространство создает новые препятствия и затруднения. Кибербезопасность влияет на каждого человека, входящего в контакт, а из-за растущей зависимости от ИКТ основной инфраструктуры общества, в настоящее время она касается даже тех, кто не связан с сетью. Атаки на услуги информационной инфраструктуры и интернета в настоящее время способны нанести серьезный ущерб обществу новыми способами. Благодаря уникальным характеристикам и проблемам, представляемым вооружениями для кибервойны, пригодные в прошлом стратегии поддержания мира, могут более не являться эффективными.

Сдерживание уже давно является излюбленным подходом для поддержания мира и безопасности между государствами в условиях применения вооружений, которые могут привести к массовым разрушениям. Но эффективность сдерживания зависит от определенных условий и предположений, многие из которых не применяются в киберпространстве[[186]](#footnote-186). Сдерживание обычно требует четыре ключевых элемента: определение (знание о том, кто напал на вас); место (знание о том, откуда идет нападение); ответ (возможность ответить, даже если ты первым подвергся нападению), а также прозрачность (знание врагом ваших возможностей и намерения реагировать с использованием вооруженных сил[[187]](#footnote-187)). Киберпространство и кибервойна приносят новые проблемы, которые подрывают основные предположения о том, что эти четыре элемента существуют, когда страны строят свои военные оборонительные арсеналов. ИКТ расширяет число способов, с помощью которых злоумышленник может скрыть свою личность и местонахождение; злоумышленники могут использовать проксиоборудование или такие услуги, как терминалы доступа в интернет общего пользования, беспроводные сети и предоплаченные услуги мобильной связи, которые не требуют аутентификации. Технологию шифрования, которая является ключевым техническим решением для обеспечения конфиденциальности, целостности и доступности, можно использовать также для маскировки идентификационных данных или, по крайней мере, для затруднения поисков места происхождения кибератаки. Технические процессы и правила, которые ограничивают хранение данных трафика интернет также вносят свой вклад в проблему определения личности и местоположения.

Риск того, что возмездие будет направлено против ошибочной цели, а также неопределенность побочного ущерба от киберконтрудара, который легко может причинить вред союзникам или нейтральным сторонам, еще боле сокращают возможности ответной реакции на нападение со стороны государств[[188]](#footnote-188). Если злоумышленники считают, что они могут остаться незамеченными или не верят, что их жертвы будут реагировать с применением военной силы из-за опасений отступления от международных норм, то угроза ответных действий очень слаба. Отвечая с применением военной силы на кибератаку, в которой вооруженные силы не использовались и которая была предназначена более для незаконного использования, чем для уничтожения, осуществляющая возмездие жертва рискует в том, что международное сообщество интерпретирует ее действия как агрессивные и необоснованные[[189]](#footnote-189). Стратегия сдерживания также рекомендует странам формировать в отношении друг друга угрожающие положения и изобретать новые ответные угрозы в различных областях для компенсации возможных диспропорций, развенчивая преимущества дальнейшей интеграции и роста напряженности в отношениях между странами[[190]](#footnote-190). Во всех этих способах основные характеристики киберпространство подрывают эффективность сдерживания как подхода к поддержанию кибермира.

Сами рамки существующих правовых подходов могут оказаться более не достаточными для управления рисками, связанными с кибербезопасностью. Например, в соответствии с существующим международным законом, изложенным в Статье 51 Хартии ООН, государство может законно действовать в целях самообороны, когда противостоит вооруженному нападению. В контексте кибервойны это положение, конечно, ставит новые вопросы о том, когда кибератаку можно считать равнозначной вооруженному нападению, а затем, можно ли связать эту атаку с определенным государством[[191]](#footnote-191). Казалось бы, установленная доктрина "ответственности государства" должна пролить некоторый свет на последний вопрос, он соответствует предположению, что каждое государство должно принимать меры для предотвращения того, чтобы ее территория использовалась для нападения на другие государства, и если оно отказывается принимать превентивные меры, то оно может нести ответственность за такие нападения. Однако как видно из предварительных оценок кибератак, в киберпространстве на такой практический вопрос становится бесконечно трудно ответить  некоторые атаки не имеют географических источников, например в случае с "ботнетами", они могут пересекать несколько границ и инициироваться в коалициях, расположенных в нескольких странах, или осуществляется с использованием проксиоборудования, которое лишь действует от имени реального преступника. Иногда сами государства не в состоянии обнаружить или проверить, какие стороны действуют на их собственной территории. И, даже если государство может определить сторону, действующую на ее географической территории, сама природа киберпространства делает невозможным полный контроль со стороны какого-либо отдельного субъекта[[192]](#footnote-192). Таким образом, неясным неизбежно становится не только вопрос об источнике атаки, но и вопрос о контроле.

**b) Необходимость международных рамок**

Поскольку существующие международная правовые нормы и инструменты не в полной мере пригодны для борьбы с новыми проблемами кибербезопасности, в настоящее время необходимо обсуждение и сотрудничество на глобальном уровне. Постоянно меняющийся характер самой технологии с ее расширяющимися областями пересечения между юрисдикцией и ИКТ определенной страны, онлайновыми ресурсами и системами, придает принятию нового набора стратегий и международному сотрудничеству еще большее значение для обеспечения кибермир[[193]](#footnote-193).

Кибератаки могут возникать и происходить в любой точке мира, что делает эти угрозы по своей сути международными, и для адекватного противостояния им требуется международное сотрудничество, взаимопомощь в расследованиях, а также общие материально-правовые и процессуальные нормы. Кроме того, международное сотрудничество уже широко признается одним из ключевых требований обеспечения глобальной кибербезопасности. В 2003 и 2005 годах на Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО) страны согласились с необходимостью создания эффективных и действенных средств, как на национальном, так и на международном уровне в целях содействия сотрудничеству в области международной кибербезопасности[[194]](#footnote-194). Это международное сотрудничество должно быть мотивировано не только взаимным стремлением к миру, но и подчеркнутыми личными интересами каждой страны. В настоящее время каждая страна в решающей степени зависит от технологии для торговли, финансов, здравоохранения, служб экстренной помощи, распределение продовольствия и многого другого. Потеря жизненно важных сетей может осложнить жизнь любой страны, и никто не застрахован от кибератаки. Таким образом, первостепенное значение ИКТ и взаимосвязанность развивающихся технологий формируют новый мировой порядок, который требует сотрудничество по новым вопросам в целях обеспечения стабильности.

Очень важно, чтобы страны гармонизировали свои правовые рамки по борьбе с киберпреступностью и упрощения динамичного, многогранного международного сотрудничества. Государства должны работать над созданием общей нормативно-правовой и регуляторной базы, а также создать систему для регулярного обновления этих законов, с тем чтобы они учитывали постоянно меняющийся характер угроз безопасности. Некоторые группы уже призывают к обнародованию международных стандартов и кибернорм как способу повышения международной кибербезопасности[[195]](#footnote-195). В любом случае, эффективная стратегия для поддержания кибермира должна быть гибкой и достаточно адаптивной, чтобы ее управление реагировало на быстрые темпы технического прогресса, рост ИКТ и сопутствующих проблем безопасности. Страны также должны согласовать процедуры и подходы к вопросам отслеживания источников и идентификационных данных в целях борьбы с анонимными кибератаками и международными угрозами, которые они угрожают создать. Предложения по международному соглашению требуют, чтобы каждая страна определила свои правила работы в киберпространстве для решения проблемы определения, привязывание ответственности к географической точке местоположения источника атаки может обойти неясный пока процесс определения того, кто именно организовал кибератаку[[196]](#footnote-196). Однако эти предложения оставляют нерешенными проблемы выявления проксиоборудования и отслеживания атак в их географическом местоположении, то есть в правильной точке источника атаки. Учитывая недостатки традиционных и существующих подходов к международной безопасности, ясно, что мировое сообщество должно принять новую стратегию для решения проблем кибербезопасность и обеспечение прочного кибермира.

## 7.4 Предложения в текст Международных принципов в киберпространстве

Пропагандируя руководящие принципы для поддержания кибермира, мы должны учитывать отличительные характеристики киберпространства и проблемы наиболее для них характерные. Однако мы можем обратиться к другим движениям, направленным на борьбу с аналогичными транснациональными угрозами, таких как Конвенция против транснациональной организованной преступности, для того чтобы сообщить о наших подходах. Так же как и транснациональная организованная преступность, кибератаки стирают государственные границы и действуют через сложные сети, которые идут параллельно мирным системам производства или накладываются на них. Конвенция иллюстрирует общее понимание того, что эти широко распространенные, транснациональные проблемы должны решаться в тесном международном сотрудничестве и что они требуют принятия новых концепций, взаимной правовой помощи и содействия развитию, обмена информацией и сотрудничества правоохранительных органов[[197]](#footnote-197).

Известная правовая доктрина и одобренные на международном уровне нормы поддерживают определенные необходимые элементов плана создания кибермира. В частности, Статья 19 Всеобщей Декларация о правах человека предусматривает право на свободу убеждений и их выражение, которое включает в себя свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ[[198]](#footnote-198). В своем Женевской Декларация принципов 2003 года, Всемирная встреча на высшем уровне по вопросам информационного общества (ВВУИО) подтвердила, что понятие свободы общения является важной основой информационного общества[[199]](#footnote-199). Декларация далее подчеркивается роль общения как основополагающего социального процесса и основной потребностью человека, которая служит фундаментом любой общественной организации. Соответственно, все люди должны иметь равный доступ к информационным и коммуникационным технологиям. Организация Объединенных Наций выразила свое обязательство по обеспечению этого доступа для всех, и с полномасштабным использованием для этого потенциала цифровой революции[[200]](#footnote-200).

Хотя различия между ядерными материалами и ИКТ огромны, несколько ключевых аналогий делают международное сотрудничество по обеспечению ядерного мира учебником стратегии кибермира. Так же как киберпространство и ИКТ, ядерная энергия и технологии могу использоваться как в мирных, так и в военных целях, они способны производить массовые разрушения при использовании в целях нападения и, в то время как они будут использованы против одной страны, влияние таких атак ощутят все страны[[201]](#footnote-201). Признавая глобальный, по своей сути, характер угрозы ядерного нападения, международное сообщество стремится создать многостороннюю совместную стратегию, которая предполагает наличие единого подхода и общего стремления к ядерной безопасности[[202]](#footnote-202). Такие договора, как Договор о нераспространении ядерного вооружения (ДНЯО) иллюстрируют эффективный подход к проблеме сохранения мирного использования потенциально разрушительного материала, способного пересекать национальные границы. ДНЯО возлагает ответственность за материалы на основе территориальной юрисдикции или деятельности, "осуществляемой под контролем [государства] в любом месте"[[203]](#footnote-203). Разделяя такой подход, в 2010 году на саммите по ядерной безопасности сорок семь стран подтвердили свою приверженность обеспечению безопасности ядерных материалов, находящихся под их контролем, в целях дальнейшего повышения безопасности при изменении условий и обмена передовым опытом и практическими решениями для безопасности[[204]](#footnote-204).

ДНЯО также подчеркивает преимущества мирного применения ядерных технологий и важность того, чтобы эти преимущества были бы доступными для всех государств, включая развивающиеся страны[[205]](#footnote-205). Договор подчеркивает важность международного сотрудничества всех стран, включая обмен информацией и материалами для внесения вклада в дальнейшее развитие мирного использования атомной энергии[[206]](#footnote-206). Кроме того, Статья 3 ДНЯО связывает страны, его подписавшие, определенными обязательствами по обеспечению безопасности, которые направлены на предотвращение изменение использования ядерной энергии с мирного применения на ядерное оружие или другие разрушительные применения[[207]](#footnote-207). Международное агентство по атомной энергии, признанное за свой опыт, знания и способности в том, чтобы способствовать обсуждению в рамках нейтральных форумов, взяло обязательство контролировать переговоры и заключение между государствами соглашения, которое определит такую систему гарантий[[208]](#footnote-208). Среди других форм сотрудничества по обеспечению ядерного мира отметим Глобальную инициативу по борьбе с ядерным терроризмом – международное партнерство стран, решивших работать по отдельности и совместно над созданием набора общих принципов ядерной безопасности[[209]](#footnote-209). Эти принципы включают в себя: разработку и совершенствование учета, контроля и мер по обеспечению безопасности ядерных материалов и гражданских ядерных объектов, совершенствование в странах-членах средств обнаружения и управления, предотвращения создания убежищ для террористов, улучшение ответной реакции стран-членов, смягчение последствий и улучшение возможностей расследования в случае нападения, а также улучшение обмена информацией[[210]](#footnote-210).

Международные усилия по обеспечению мира в других новых и, казалось бы, безграничных сферах также решительно содействуют широкому международному сотрудничеству. Например, Декларация правовых принципов, регулирующих деятельность государств по исследованию и использованию космического пространства, наряду с другими руководящими принципами включает в себя предположение о том, что все государства должны сотрудничать и оказывать взаимную помощь в исследовании и использовании космического пространства[[211]](#footnote-211).

Признавая, растущий риск кибератаки, которая могут возникать в любом месте и затронуть каждую страну, Генеральный секретарь МСЭ предлагает пять руководящих принципов для установления и защиты мира в зарождающейся кибервселенной. Эти принципы воплощают и продвигают ценности и культуру Международного союза электросвязи, ясно видимые на протяжении долгой истории его существования как лидера в области международной стандартизации и регулирования. Авторитетный Регламент международный электросвязи (РМЭ) МСЭ является всего лишь одним  
примером этой традиции содействия гармоничному развитию, эффективной работе и универсального доступа к международной электросвязи и технологии. РМЭ был создан как новая концепция нормативно-правовой базы для решения вопросов и проблем, сопровождающих новые условия в сфере электросвязи, проявившиеся в конце 1980-х годов[[212]](#footnote-212). Он был разработан для повышения эффективности и ускорения развития в рамках сотрудничества, взаимодействия и равного доступа, и таким образом, иллюстрирует традиции МСЭ. Он также отражает взгляд Союза на проблему защиты права на общение при условии не нанесения ущерба объектам связи.

Пять принципов кибермира Генерального секретаря МСЭ также включают в себя эти основные ценности, определяя в тоже время конкретные действия и обязательства, которые обеспечат мир и стабильность в киберпространстве. Эти принципы гласят, что:

1 Каждое правительство должно взять на себя обязательство дать своему народу доступ к средствам связи.

2 Каждое правительство возьмет на себя обязательство защищать своих людей в киберпространстве.

3 Каждая страна возьмет на себя обязательство не укрывать террористов/преступников на своих территориях.

4 Каждая страна должна взять на себя обязательство не применять первой кибератаки по отношению к другим странам.

5 Каждая страна должна взять на себя обязательство взаимодействовать с другими странами в рамках международного сотрудничества для обеспечения мира в киберпространстве.

# 8 Глобальная программа кибербезопасности МСЭ

**Хамадун И. Туре (Hamadoun I. Touré)**

МСЭ представляет собой уникальный глобальный форум для обсуждения проблем кибербезопасности. Союз играет важную роль в области электросвязи, информационной безопасности и стандартизации в различных сферах деятельности с самого момента своего основания в 1865 году, почти 145 лет назад. МСЭ понимает, что масштабы и характер задач кибербезопасности требуют скоординированных многосторонних действий, и соответствующим образом работает для достижения этой цели. В частности, МСЭ в настоящее время содействует кибербезопасности посредством ряда мероприятий в области стандартизации и технической помощи развивающимся странам с учетом их специфических потребностей. В знак признания его многолетнего опыта, потенциала и накопленных знаний, мировые лидеры и правительства назначили МСЭ единственным агентом, обеспечивающим направление деятельности С5 ВВУИО "[Укрепление доверия и безопасности при использовании ИКТ](http://www.itu.int/wsis/docs2/tunis/off/6rev1.html)"[[213]](#footnote-213). Таким образом, главы государств и другие мировые лидеры, принимающие участие в ВВУИО, а также Государства  Члены МСЭ, поручили МСЭ проложить путь путем принятия конкретных мер по сдерживанию угрозы и уменьшению неуверенности, связанных с информационным обществом. МСЭ Резолюция 140 Полномочной конференции МСЭ (Пересм. Анталия, 2006 год), обращаясь к роли МСЭ в реализации результирующих документов ВВУИО, поручила Генеральному секретарю МСЭ принять все необходимые меры для выполнения мандата МСЭ.

Соответственно, в мае 2007 года Генеральный секретарь объявил [Глобальную программу кибербезопасности (ГПК)](http://www.itu.int/osg/csd/cybersecurity/gca/index.html), которая должна создать среду, в рамках которой все заинтересованные стороны смогут координировать международную реакцию на растущие проблемы кибербезопасности. ГПК основана на международном сотрудничестве и стремится привлечь все соответствующие заинтересованные стороны к осуществлению согласованных усилий по укреплению доверия и безопасности в информационном обществе. Совсем недавно, государства-члены утвердили работу МСЭ в этой области на Полномочной конференции 2010 года, вновь подтверждая в Резолюции 130 (Пересм. Гвадалахара, 2010 год), что ГПК является основой для международного сотрудничества. Эта Резолюция поручает Генеральному секретарю продолжить рассмотрение и улучшить достигнутые результаты в рамках его компетенции. В частности, государства-члены отметили усиление роли МСЭ в укреплении доверия и безопасности в использовании ИКТ, а также глобальную инициативу Союза в сотрудничестве с Международным многосторонним партнерством против киберугроз (IMPACT) и Форумом по реагированию на инциденты и команд безопасности (FIRST). Резолюция также решает продолжать в рамках МСЭ уделять первоочередное внимание его работам, касающимся безопасности информационно-коммуникационных сетей

ГПК работает над достижением семи стратегических целей, которые включают в себя:

a) Формирование стратегии разработки типового законодательства в сфере киберпреступности, которое было бы глобально применимым и полностью совместимым существующими национальными и региональными законодательными мерами;

b) Разработку глобальных стратегий для создания соответствующих национальных и региональных организационных структур и политики в области киберпреступности;

c) Разработку стратегии создания признанных на глобальном уровне минимальных критериев безопасности и схем аккредитации для аппаратных и программных приложений и систем;

d) Разработку стратегий для создания глобальной рамочной основы для отслеживания, предупреждения и реагирования на инциденты с целью обеспечения трансграничной координации между новыми и существующими инициативами;

e) Разработку глобальных стратегий для создания и утверждения общей и универсальный цифровой системы идентификации и необходимой организационной структуры для обеспечения признания цифровых учетных данных в различных географических границах;

f) Разработку глобальной стратегии для облегчения создания человеческого и организационного потенциала с целью повышения осведомленности и распространения "ноу-хау" в различных секторах и во всех вышеупомянутых областях, а также

g) Предложения по созданию основы для глобальной многосторонней стратегии для международного сотрудничества, диалога и координации во всех вышеупомянутых областях,

Для достижения этих целей, ГПК сосредоточена на пяти основных принципах для руководства своих областях деятельности. Это следующие принципы:

1 Правовые меры

Организованная киберпреступность находится на подъеме, так как интернет оказался прибыльной бизнес ареной с низким уровнем риска. Причина этого в том, что в национальном и региональном законодательстве по-прежнему остаются пробелы, что затрудняет даже задачу эффективно отследить преступников. В структуре ГПК этот принцип заключается в разработке стратегий развития модели, применимой в глобальном масштабе и полностью совместимой с законодательством о киберпреступности. В частности, имея различными ресурсы законодательства о киберпреступности, МСЭ помогает государствам-членам понять правовые аспекты кибербезопасности, с тем чтобы гармонизировать свои правовые рамки.

2 Технические и процедурные меры

Этот принцип сосредоточен на мерах по устранению уязвимостей программных продуктов с целью разработки глобально приемлемых схем, протоколов и стандартов аккредитации. МСЭ и, в частности Сектор стандартизации МСЭ (МСЭ-Т) и Сектор радиосвязи МСЭ (МСЭ-R), занимают уникальную позицию в области стандартизации ИКТ, а также играет важную роль в разрешении проблем безопасности для уязвимостей в протоколах. В целях выявления киберугроз и разработки контрмер для снижения рисков, МСЭ работает над усовершенствованием защищенных услуг связи, пересматривает спецификации по безопасности для сквозной мобильной передачи данных и рассматривает требования безопасности для веб-услуг и прикладных протоколов. Оперативные группы и Исследовательские комиссии МСЭ, такие, как недавно созданная Оперативная группа по интеллектуальным энергосистемам, являются эффективным механизмом для достижения этих целей.

3 Организационные структуры

Мир уже осознал, что системы мониторинга и предупреждения, а также и реагирование на инциденты имеют большое значение, когда речь идет о реагировании на кибератаки, также как и свободный поток информации, взаимодействие и сотрудничество внутри национальных организационных структур и между ними. Следовательно, этот принцип направлена на создание организационных структур и стратегий для предотвращения, обнаружения и реагирования на атаки против важнейших информационных инфраструктур. В этой связи МСЭ работает с государствами-членами над тем, чтобы определить их конкретные потребности в области кибербезопасности и оказать им необходимую помощь в создании национальных команд реагирования на компьютерные инциденты (CIRT). Кроме того, в рамках сотрудничества МСЭ с Международным многосторонним партнерством против киберугроз (IMPACT), ключевую роль в реализации целей ГПК играет Глобальный центр реагирования (GRC).

МСЭ и IMPACT официально подписали Меморандум о взаимопонимании, посредством которого оборудованная по последнему слову техники штаб-квартира IMPACT в Сайберджая, Малайзия, по сути, стала физическим домом для ГПК. Это сотрудничество дает 192 государствам  членам МСЭ опыт, средства и ресурсы для эффективного решения проблем наиболее серьезных мировых киберугроз. Тесное взаимодействия между пятью областями работы ГПК и услугами и инфраструктурой, предоставленной IMPACT, сделали это партнерство логичным шагом в глобальной борьбе против киберугроз. Около шестидесяти стран уже присоединились к сотрудничеству[[214]](#footnote-214).

IMPACT предоставляет ресурсы для экстренного реагирования в целях содействия выявлению киберугроз и совместного использования ресурсов для оказания помощи государствам-членам[[215]](#footnote-215). Глобальный центр реагирования (GRC) оснащен самым современным ИТ и телекоммуникационным оборудованием для работы в кризисной ситуации, полнофункциональным оперативным центром, постоянно находящимся в боевой готовности, полностью резервируемым защищенным центром обработки данных, средствами для вахтовой работы сотрудников, собственным центром радиовещания и смотровой галереей для VIP персон. Таким образом, GRC играет ключевую роль в реализации цели ГПК по введению технических мер для борьбы с новыми и развивающимися киберугрозами. Двумя основными моментами GRC являются Сеть раннего предупреждения (NEWS) и Прикладная платформа электронного взаимодействия для экспертов (ESCAPE). Программа NEWS помогает странам-членам выявить киберугрозы на раннем этапе и дает необходимое руководство о том, какие меры следует принять для их устранения. Программа ESCAPE является одним из специализированных инструментов и систем, к которой будут иметь доступ государства члены. ESCAPE это  электронный инструмент, который позволяет уполномоченным киберэкспертам из разных стран объединять ресурсы и взаимодействовать друг с другом удаленно, оставаясь в безопасной и надежной окружающей среде. В короткие сроки, объединяя ресурсы и опыт разных стран, ESCAPE позволит отдельным странам и мировому сообществу незамедлительно реагировать на киберугрозы, особенно в кризисных ситуациях

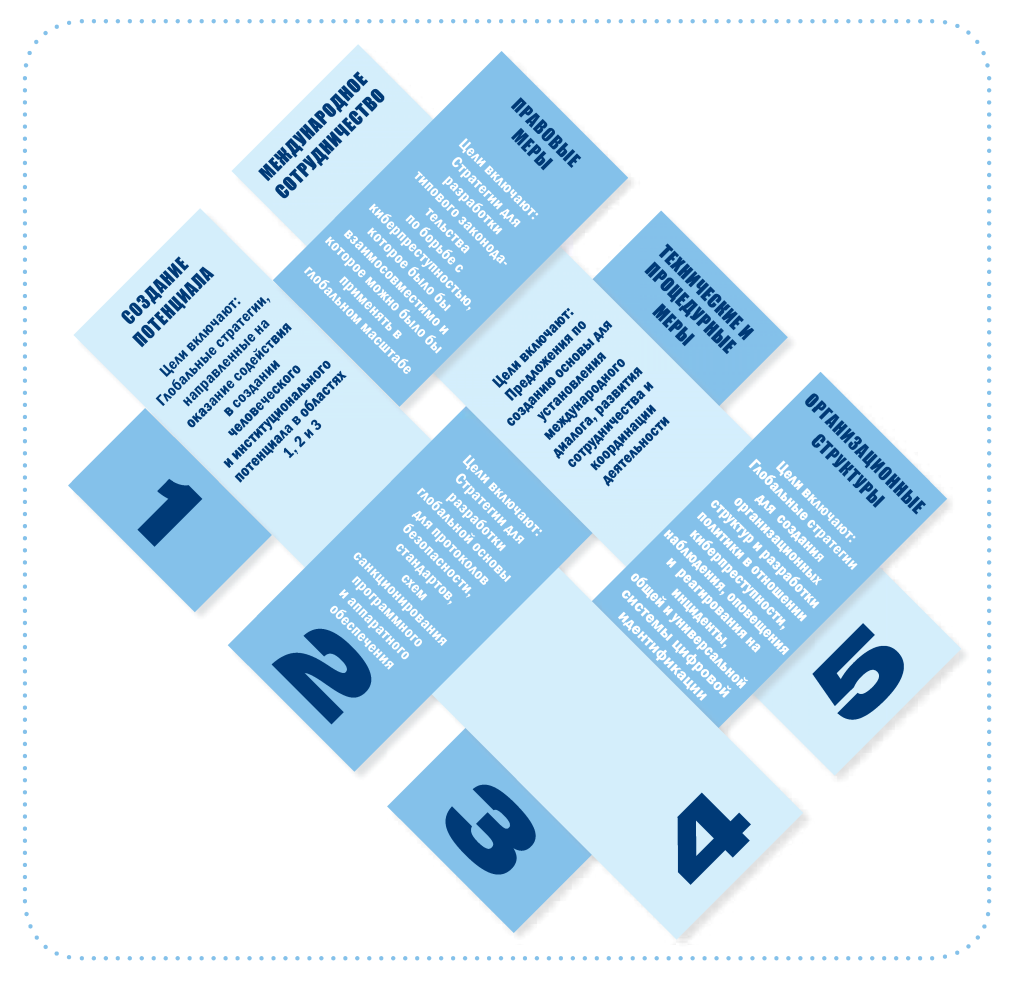
Мало того, что цели и ресурсы, предоставляемые в ходе этого сотрудничества, соответствуют пяти принципам ГПК, они также тесно связаны с предлагаемыми принципами кибермира. Ресурсы, предоставленные партнерством IMPACT государствам-членам, будет помогать каждому правительству защищать свой народ от кибератак, гарантируя им, таким образом, постоянный доступ к связи через интернет и другие ИКТ. Присоединившись IMPACT и участвуя в совместном использовании ресурсов и обсуждениях с другими государствами-членами, каждое государство будет также активно осуществлять Пятый принцип  приверженность к сотрудничеству в международных рамках для обеспечения кибермира. Кроме того, IMPACT также предлагает стипендии, дающие право развивающимся странам-членам посещать учебные курсы, которые будут сосредоточены на создании пула ресурсов и приобретенных знаний, которыми слушатели смогут поделиться с другими с целью создания национального потенциала и приобретения опыта в области кибербезопасности. Эти стипендии повысят способность каждой страны обеспечить безопасность своих ресурсов ИКТ, а также обеспечат доступ к своему собственному народу

4 Создание потенциала

В рамках ГПК, этот принцип заключается в разработке стратегий для повышения осведомленности и распространения опыта в целях усиления позиций кибербезопасности в повестке дня национальной политики. Потребности в создании потенциала должны удовлетворяться в целях развития устойчивой и активной культуры кибербезопасности. Понимание и осведомленность о потенциальных опасностях в киберпространстве являются критическими, если конечный пользователь должен пользоваться преимуществами ИКТ безопасно. В частности, в соответствии с мандатам МСЭ по оказанию помощи государствам-членам в разработке функциональных возможностей кибербезопасности, МСЭ работает, над тем, чтобы содействовать внедрению и развертыванию возможностей кибербезопасности, таких, как Руководство МСЭ по национальный кибербезопасности, Ресурсы киберпреступности МСЭ и Инструментарий МСЭ по смягчения действий ботнетов.

5 Международное сотрудничество

Кибербезопасность является такой же глобальный и далеко идущей, как и интернет. Следовательно, пятый принцип ГПК сфокусирован на стратегии международного сотрудничества, диалога и координации. Взаимодействие с IMPACT представляет собой значительный прогресс в этом направлении, предоставляя государствам-членам и третьим сторонам платформу для обсуждения политики и обмена информацией. Это действие непосредственно расширяет мандат МСЭ, полученный им от широкого круга государств-членов в соответствии с направлением действий С5ВВУИО. Декларация принципов ВВУИО гласит, что укрепления основы для доверия, в том числе информационная и сетевая безопасность, аутентификация, конфиденциальность и защита прав потребителей, являются предпосылкой для развития информационного общества и роста доверия со стороны пользователей ИКТ. Для того чтобы добиться этого, необходимо в сотрудничестве со всеми заинтересованными сторонами и международными экспертными органами активно формировать, развивать и внедрять глобальную культуру кибербезопасности. Сотрудничества с IMPACT, в дополнение к РМЭ МСЭ и оперативным группам, укрепляет эту основу для доверия и работает на достижение этих целей, используя комплексный подход и предоставление места встречи для всех членов мирового сообщества.



Глобальная программа кибербезопасности: пять стратегических принципов

**Заключение**

Хотя угрозы, сопровождающие киберразвитие, и усиление зависимости от ИКТ являются серьезными, потенциальные выгоды еще более убедительны. Хотя мы видим, что некоторые из рисков кибервойны уже пришли в нашу жизнь, мы также уже получаем выгоды от киберпространства, а возможности для будущих выгод бесконечны. По мере продвижения вперед, мы должны рассмотреть вопрос о том, как мы можем продолжать существовать в условиях растущей киберзависимости, развития и интеграции, а также о том, как мы можем защитить ресурсы, создать стабильные условия для дальнейшего расцвета инфраструктуры и новых технологий, и обеспечить прочный мир. Хотя многие существующие подходы представляют собой позитивные шаги, они не отвечают требуемому уровню и не могут обеспечить наиболее эффективное решение. Но имеется большая вероятность, что если мы будем работать вместе, мы можем достичь этих целей и избежать тяжелых последствий киберконфликта. МСЭ уже эффективно работает в этом направлении различными способами, и он держит в руках ресурсы и влияние, необходимые для содействия необходимой многосторонней поддержки и участия.

# 9 Декларация Эриче по принципам киберстабильности и кибермира

**Всемирная федерация ученых (World Federation of Scientists)**

## Декларация Эриче по принципам киберстабильности и кибермира

*Беспримерным триумфом науки является то,* что человечество, используя современные информационно-коммуникационные технологии (ИКТ), теперь имеет средства для расширения экономических ресурсов для всех стран, для увеличения интеллектуальных возможностей своих граждан и для развития их культуры и доверия к другим сообществам. Интернет, как и сама наука, является по своей природе в основном транснациональным и повсеместным. Интернет и его сопутствующие информационные инструменты, является необходимым ресурсом научного обсуждения на национальном и международном уровне, предлагая всем возможность воспользоваться открытой наукой, без секретов и без границ.

В двадцать первом веке интернет и другие взаимосвязанные сети (киберпространство) стали крайне важны для благосостояния человека, политической независимости и территориальной целостности национальных государств.

*Опасностью является то,* что в мире сильно вырос уровень взаимосвязей, а риски и угрозы стали настолько сложны и всеобъемлющи, что их уровень растет в геометрической прогрессии по сравнению с возможностью противостоять им. Теперь для национальных государств или злоумышленников существует возможность нанести серьезный вред жизни и обществу во всех странах; киберпреступления и их результат, киберконфликты, угрожают мирному существованию человечества и полезному использованию киберпространства.

Информационно-коммуникационные системы сети поддерживают национальную и экономическую безопасность во всех странах и служат в качестве центральной нервной системы для возможности отклика, действий на деловом и правительственном уровне, социальных служб, общественного здравоохранения и личного благосостояния.

Информационные инфраструктуры и системы становятся очень важны для здравоохранения, безопасности и благосостояния человека, особенно для пожилых, нетрудоспособных, немощных людей и детей. Значительные разрушения в киберпространстве могут привести к нежелательным страданиям и разрушениям.

ИКТ поддерживают принципы прав человека, обеспечиваемые международным законодательством, включая *Всемирную Декларацию прав человека* (Статьи 12, 18 и 19) и *Международный пакт о гражданских и политических правах* (Статьи 17, 18, и 19). Разрушение киберпространства (a) негативно отражается на правах человека на частную, семейную жизнь, на право иметь дом и общаться без помех или атак, (b) создает помехи правам на свободу мысли, совести и вероисповедания, (c) ограничивает право на свободу убеждений и выражений и (d) ограничивает право на получение и передачу информации и идей в любой среде передачи и вне зависимости от границ.

ИКТ могут стать инструментом для совершения благих дел или нанесения вреда, и потому также являются инструментом построения мира или создания конфликтов. Для того чтобы пользоваться преимуществами информационного века необходимо, чтобы информационные сети и системы были устойчивыми, надежными, доступными и проверенными. Гарантии целостности, безопасности и стабильности киберпространства в целом требуют согласованных международных действий.

**ПОЭТОМУ мы рекомендуем следующие принципы для достижения и поддержки киберстабильности и кибермира:**

1 Все правительства должны понимать, что международное право гарантирует людям свободную передачу информации и идей; эти гарантии также распространяются на киберпространство. Ограничения должны вводиться только в виде необходимой меры и сопровождаться процессами, позволяющими провести правовую экспертизу.

2 Все страны должны работать вместе для создания общего кодекса поведения в киберпространстве и создания согласованной всемирной правовой инфраструктуры, включая процессуальные нормы в отношении содействия и сотрудничества в области расследований, действующих в рамках конфиденциальности и прав человека. Все правительства, поставщики услуг и пользователи должны поддерживать международную деятельность по обеспечению правопорядка в области киберпреступлений.

3 Все пользователи, поставщики услуг и правительства должны работать над тем, чтобы гарантировать то, что киберпространство не будет использоваться любым способом, который может привести к эксплуатации пользователей, особенно юных и беззащитных, посредством насилия и ущемления прав.

4 Правительства, организации и частный сектор, включая отельных граждан, должны внедрять и поддерживать всесторонние программы безопасности на основе примеров передового опыта и стандартов на международном уровне и использовать технологии обеспечения конфиденциальности и безопасности.

5 Создатели программного обеспечения и оборудования должны стремиться разработать безопасные технологии, которые обеспечивают способность к восстановлению функций и сопротивление к уязвимым местам.

6 Правительства должны активно участвовать в программах Организации Объединенных Наций по обеспечению глобальной кибербезопасности и кибермира и для избежания использования киберпространства в конфликтах.

*Проект Декларации Эриче по принципам киберстабильности и кибермира был создан Постоянной группой по мониторингу Всемирной федерации ученых (WFS), Женева, и утвержден на Пленарном заседании WFS по случаю 42-ой Сессии Международных семинаров по вопросучрезвычайных ситуаций глобального масштаба в Эриче (Сицилия) 20 августа 2009 года.*

# 10 Заключение

**Джоди Р. Вестбай (Jody R. Westby)**

На сегодняшний день поиски кибермира велись на удивление тихо. Постоянная группа экспертов по мониторингу информационной безопасности Всемирной федерации ученых первая выдвинула концепцию кибермира в программе семинаров, которые она представила в Папской академии наук Ватикана в декабре 2008 года. Впоследствии в 2009 году, PMP подготовила проект "Декларации Эриче о принципах киберстабильности и кибермира", которая была принята WFS и распространен среди всех членов Организации Объединенных Наций. Концепции и принципы, сформулированные в настоящей публикации, отражают отрезвляющую оценку PMP в том, что мир мчится к киберхаос, но путь к кибермиру приведет к повышению глобальной стабильности.

Статистические данные и сценарии, представленные здесь, показывают серьезность киберпреступлений и киберконфликтов. Интернет создал "преступление на выбор", потому определение автора затруднено, а преступников редко ловят и предают суду. Мы опасаемся, что интернет также становится излюбленным оружием. Благодаря быстрому доступу к наиболее важным данным страны и инфраструктуре критических операций, самая маленькая страна может победить страны с крупнейшими оборонными бюджетами. Развивающиеся страны показали, развитым странам, как построить нелинейную инфраструктуру ИКТ с использованием спутниковых и беспроводных технологий. Кроме того, страны начинают понимать, что киберсреда дает привлекательную нелинейную возможность продвижения национальных и экономических интересов в области безопасности

Почему киберсдерживания или кибермир не являются мантрой сегодняшнего дня? Вместо этого военные лидеры во всем мире очень заняты, объявляя о создании киберкоманд и их планов по развитию возможностей для атаки, защиты и использования сети. Когда страны сталкиваются с ядерным оружием, они начали требовать сдерживания и нераспространения. Страны по всему миру объединились с общей целью остановить глобальную опасность, которая угрожает человечеству. Как показали эстонская и грузинская атаки, когда нападающая страна сталкивается с недостаточностью международной правовой базы, дипломатической неопределенностью, техническими ограничениями и невозможностью слежения и связи, понятие кибермир становится весьма привлекательным

Хотя многие многонациональные организации работают над различными аспектами киберпреступности и/или киберконфликта, только МСЭ принял глобальный взгляд и выдвинул повестку дня, предназначенную для решения основных проблемных областей, используя при этом усилия других организаций. Генеральному секретарю следует отдать должное за его руководство, видение и мужество, требуемое чтобы решать такие огромные проблемы в лоб. Мы искренне надеемся, что другие организации одобрят этот подход и будут подражать ему, и что лидеры продвинутся вперед в разработке кодекс киберповедения и правовой основы, поддерживающих и продвигающих геокиберстабильность.

Мы приближаемся к опасной пропасти, в это время темная сторона интернета может затмить огромные выгоды ИКТ и расстроить мировой порядок. Время для кибермира сейчас!

1. Термин "киберконфликт" включает в себя сценарии, которые можно обозначить как "кибервойны". [↑](#footnote-ref-1)
2. "A Brief History of the Net," *Fortune*, 9 Oct. 2000 at 34, [http://money.cnn.com/magazines/  
   fortune/fortune\_archive/2000/10/09/289297/index.htm](http://money.cnn.com/magazines/fortune/fortune_archive/2000/10/09/289297/index.htm) (далее "Fortune"); *смотрите также* Dave Krisula, "The History of the Internet," Aug. 2001 (expanded 2009), [www.davesite.com/  
   webstation/net-history1.shtml](http://www.davesite.com/webstation/net-history1.shtml) (далее "Krisula"). [↑](#footnote-ref-2)
3. Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, "A Brief History of the Internet," Internet Society (ISOC) All About the Internet, [www.isoc.org/internet/history/brief.shtml](http://www.isoc.org/internet/history/brief.shtml) (далее "A Brief History of the Internet"); Ликлидер опубликовал свои записки "Галактическая сеть" в августе 1962 года и начал работать в ARPA в октябре 1962 года. [↑](#footnote-ref-3)
4. Krisula; *смотрите также* Fortune; Stewart Brand, "Founding Father," *Wired*, Mar. 2001 at 148, [www.wired.com/wired/archive/9.03/baran\_pr.html](http://www.wired.com/wired/archive/9.03/baran_pr.html) (далее "Brand"). [↑](#footnote-ref-4)
5. Brand at 145153; *смотрите также* Krisula. [↑](#footnote-ref-5)
6. A Brief History of the Internet; *смотрите также* Brand at 146; Krisula. [↑](#footnote-ref-6)
7. A Brief History of the Internet. [↑](#footnote-ref-7)
8. Elizabeth D. Hoover, "The Inventor of the World Wide Web," *AmericanHeritage.com,* 12 Nov. 2005, [www.americanheritage.com/articles/web/20051112-internet-world-wide-web-tim-berners-lee-computer-geneva-cern-enquire-html-url-world-wide-web-consortium.shtml](http://www.americanheritage.com/articles/web/20051112-internet-world-wide-web-tim-berners-lee-computer-geneva-cern-enquire-html-url-world-wide-web-consortium.shtml). [↑](#footnote-ref-8)
9. "Life on the Internet: Net Timeline," PBS, [www.pbs.org/opb/nerds2.0.1/timeline/](http://www.pbs.org/opb/nerds2.0.1/timeline/); *смотрите также* Krisula. [↑](#footnote-ref-9)
10. Геополитика определяется как "1) Изучение взаимосвязи между политикой и географией, демографией и экономикой, особенно в отношении внешней политики страны, 2) а. Государственная политика использующая геополитику. b. Нацистская доктрина, утверждающая, что географические, экономические и политические потребности Германии оправдывают ее вторжение и захват других земель, 3) Сочетание географических и политических факторов, связанных со страной или регионом или влияющих на них. "Американский словарь наследия, 2000, [www.dictionary.com/search?q=geo-political](http://www.dictionary.com/search?q=geo-political). [↑](#footnote-ref-10)
11. Впервые представлена на конференции института ANSER по безопасности Отчизны "Homeland Security 2005: Charting the Path Ahead," Университет Мэриленд, Презентация Jody Westby, " A Shift in Geo-Cyber Stability and Security," 6–7 May 2002. [↑](#footnote-ref-11)
12. Steven Elliot, "Analysis on Defense and Cyberwars," *Infosec Island*, 8 July 2010, <https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html> (далее "Elliot"). [↑](#footnote-ref-12)
13. Ellen Messmer, "Cyberattack Seen as Top Threat to Zap U.S. Power Grid," *NetworkWorld*, 2 June 2010, [www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html](http://www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html) (сообщает, что угроза скоординированной кибератаки, которая может быть скомбинирована с физической атакой, считается наиболее опасной угрозой с "большим низкочастотным воздействием" для Североамериканской энергосети) (далее "Messmer"). [↑](#footnote-ref-13)
14. Thomas Claburn, "Under Cyberattack, Georgia Finds ‘Bullet-Proof’ Hosting With Google And Elsewhere," *InformationWeek*, 12 Aug. 2008, [www.informationweek.com/  
    news/security/attacks/showArticle.jhtml?articleID=210002702](http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210002702). [↑](#footnote-ref-14)
15. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," Wired, 21 Aug. 2007, [www.wired.com/politics/security/magazine/15-09/ff\_estonia?currentPage=all](http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all). [↑](#footnote-ref-15)
16. Choe Sang-Hun and John Markoff, "Cyber attacks Jam Government and Commercial Web Sites in U.S. and South Korea," *The New York Times*, 8 July 2009, [www.nytimes.com/2009/07/09/technology/09cyber.html](http://www.nytimes.com/2009/07/09/technology/09cyber.html); Jack Date, Jason Ryan, Richard Sergay, and Theresa Cook, "Hackers Launch Cyberattack on Federal Labs," ABC News, 7 Dec. 2007, <http://abcnews.go.com/TheLaw/Technology/story?id=3966047&page=1>. [↑](#footnote-ref-16)
17. Michael Mylrea. "Brazil’s Next Battlefield: Cyberspace," *Foreign Policy Journal*, 15 Nov. 2009, <http://foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace> (далее "Mylrea"). [↑](#footnote-ref-17)
18. *Id*. [↑](#footnote-ref-18)
19. Andrew Jacobs and Miguel Helft,"Google, Citing Attack, Threatens to Exit China," *The New York Times*, Jan. 12, 2010, [www.nytimes.com/2010/01/13/world/asia/13beijing.html](http://www.nytimes.com/2010/01/13/world/asia/13beijing.html). [↑](#footnote-ref-19)
20. Eliot Van Buskirk. "Denial-of-Service Attack Knocks Twitter Offline (Updated)," Wired.com, 6 Aug. 2009, [www.wired.com/epicenter/2009/08/twitter-apparently-down/](http://www.wired.com/epicenter/2009/08/twitter-apparently-down/). [↑](#footnote-ref-20)
21. *Смотрите* Abraham D. Sofaer and Seymour E. Goodman, *The Transnational Dimension of Cyber Crime and Terrorism*, 2001 at 14, <http://media.hoover.org/documents/0817999825_1.pdf>. [↑](#footnote-ref-21)
22. *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, United States Government Accountability Office, Sept. 2007, GAO-07-1036, [www.gao.gov/new.items/d071036.pdf](http://www.gao.gov/new.items/d071036.pdf). В 1997 г. (хакеры атаковали аэропорт Ворчестера в США, отключив телефоны в башне аэропорта и систему управления огнями взлетно-посадочных полос). [↑](#footnote-ref-22)
23. Elliot. [↑](#footnote-ref-23)
24. Joshua Pennell, "Securing the Smart Grid: The Road Ahead," at 2, *NetworkSecurityEdge.com*, 5 Feb. 2010, [www.networksecurityedge.com/content/securing-smart-grid-road-ahead](http://www.networksecurityedge.com/content/securing-smart-grid-road-ahead). [↑](#footnote-ref-24)
25. Elliot. [↑](#footnote-ref-25)
26. "Smart Grid," U.S. Department of Energy, www.oe.energy.gov/smartgrid.htm; "SCADA," *TopBits.com*, [www.tech-faq.com/scada.html](http://www.tech-faq.com/scada.html) (далее "SCADA"). [↑](#footnote-ref-26)
27. SCADA. [↑](#footnote-ref-27)
28. Katie Fehrenbacher, "10 Things to Know About Smart Grid Security," 9 Oct. 2009, Earth2Tech, Gigaom, <http://gigaom.com/cleantech/10-things-to-know-about-smart-grid-security/>, (далее "Fehrenbacher"}. [↑](#footnote-ref-28)
29. *Id*. [↑](#footnote-ref-29)
30. "SCADA Security and Terrorism: We’re Not Crying Wolf," at 26, BlackHat, www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf. [↑](#footnote-ref-30)
31. Siobhan Gorman. "Electricity Grid in U.S. Penetrated By Spies," *The Wall Street Journal,* 8 Apr. 2009, http://online.wsj.com/article/NA\_WSJ\_PUB:SB123914805204099085.html. [↑](#footnote-ref-31)
32. Ellen Messmer. "‘Cyberwar’ author: U.S. needs radical changes to protect against attacks," *NetworkWorld*, 7 Apr. 2010, [www.networkworld.com/news/2010/040710-clarke-book-review.html](http://www.networkworld.com/news/2010/040710-clarke-book-review.html) (далее "Radical Change"). [↑](#footnote-ref-32)
33. *Id.* (reporting that the U.S. electric power grid already endures hundreds of thousands of probes per day); Fehrenbacher (сообщает, что the 40 million smart meters installed globally have already seen a number of security breaches). [↑](#footnote-ref-33)
34. Messmer. [↑](#footnote-ref-34)
35. Mylrea. [↑](#footnote-ref-35)
36. "Cyberwar: War in the fifth domain," 7 Jan. 2010, *The Economist*, [www.economist.com/node/16478792](http://www.economist.com/node/16478792) (далее "Fifth Domain"). [↑](#footnote-ref-36)
37. *Smart Grid: Hardware and Software Outlook*, Zpryme, 2009 at 2, www.zpryme.com/SmartGridInsights/2010\_Smart\_Grid\_Hardware\_Software\_Outlook\_Zpryme\_Smart\_Grid\_Insights.pdf (сообщает, что индустрия интеллектуальных энергосетей США в 2009 году оценивалась в 21,4 миллиарда долларов США и к 2014 году ее стоимость достигнет примерно 42,8 миллиарда долларов США); Jonathan Weisman and Rebecca Smith,"Obama Trumpets Energy Grants," *The Wall Street Journal*, 28 Oct. 2009, [http://online.wsj.com/  
    article/SB125663945180609871.html](http://online.wsj.com/article/SB125663945180609871.html) (сообщает о сделанном Президентом Обамой объявлении о стимулирующих грантах в 3,4 миллиарда долларов США для новейших проектов интеллектуальных энергосетей). [↑](#footnote-ref-37)
38. Fifth Domain. [↑](#footnote-ref-38)
39. *Смотрите, например*, *Id.* (сообщает, что "наиболее вероятным вариантом использованием кибероружия будет, по всей видимости, не создание электронного апокалипсиса, а лишь как инструмент ограниченного боя"). [↑](#footnote-ref-39)
40. *Id.* [↑](#footnote-ref-40)
41. *CERT Research 2006 Annual Report*, Carnegie Mellon University, Software Engineering Institute, at 7 *et seq*., [www.cert.org/archive/pdf/cert\_rsch\_annual\_rpt\_2006.pdf](http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf). [↑](#footnote-ref-41)
42. *Understanding Cybercrime: A Guide for Developing Countries*, at 72, International Telecommunication Union, April 2009, [www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf](http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf) (далее "Understanding"). [↑](#footnote-ref-42)
43. *Trust in the Information Society: A Report of the Advisory Board RISEPTIS,* [www.think-trust.eu/](http://www.think-trust.eu/); David-Olivier Jaquet-Chiffelle*,* ed.*, Identity Revolution: Multidisciplinary Perspectives,* FIDIS, May 2009, [www.fidis.net/resources/identity-revolution/](http://www.fidis.net/resources/identity-revolution/). [↑](#footnote-ref-43)
44. См. также Kertu Ruus, "Cyber War I: Estonia attacked from Russia," *European Affairs*, Vol.9, No1-2, 2008, <http://findarticles.com/p/articles/mi_7054/is_1-2_9/ai_n28550773/>. [↑](#footnote-ref-44)
45. Kieron O’Hara*,* Trust: From Socrates to Spin, Icon Books, Cambridge, 2004 at page 10, <http://eprints.ecs.soton.ac.uk/9361/>. [↑](#footnote-ref-45)
46. Niklas Luhmann, *"Trust: A Mechanism for the Reduction of Social Complexity", Trust and Power*, New York: Wiley, 1979 at 4-103. [↑](#footnote-ref-46)
47. Russell Hardin, *Trust and Trustworthiness*; Russell Sage Foundation Series on Trust, Vol. 4, 2002. [↑](#footnote-ref-47)
48. Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity*, Free Press, 1995 [↑](#footnote-ref-48)
49. Robert D. Putnam, Robert Leonardi, and Raffaella Y. Nanetti, *Making Democracy Work: Civic Traditions in Modern Italy,* Princeton University Press, 1993 [↑](#footnote-ref-49)
50. Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?" Boston University Law Review, Vol. 81, No. 3, June 2001 at 635-664, [www.nyu.edu/projects/nissenbaum/main\_cv.html](http://www.nyu.edu/projects/nissenbaum/main_cv.html) . [↑](#footnote-ref-50)
51. "The Others," *The Economist*, 17 Dec. 2009, [www.economist.com/node/15108690](http://www.economist.com/node/15108690). [↑](#footnote-ref-51)
52. *Id.* [↑](#footnote-ref-52)
53. *См.* Nissenbaum. [↑](#footnote-ref-53)
54. Виталий Цыгичко является ассоциированным членом группы PMP InfoSecur и принимал участие в обсуждениях. [↑](#footnote-ref-54)
55. Kim Cameron, Reinard Posch, and Kai Rannenberg, *Proposal for a Common Identity Framework: A User-Centric Identity Metasystem,* Joint ‘ICT Security’ – ‘ICT for Government and Public Services’ Workshop on "Identity Management in the Future Digital Society, 14 Oct. 2008, [www.identityblog.com/?p=1048](http://www.identityblog.com/?p=1048). [↑](#footnote-ref-55)
56. "About the FIDIS Network of Excellence," [www.fidis.net/about/](http://www.fidis.net/about/). [↑](#footnote-ref-56)
57. Автор хотел бы выразить признательность за вклад Удо Хельмбрехта (Udo Helmbrecht) и его команды из ENISA (Европейского Агентства по сетевой и информационной безопасности). [↑](#footnote-ref-57)
58. "McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property," McAfee Press Release, Feb. 2010, [www.mcafee.com/us/about/press/corporate/2009/  
    20090129\_063500\_j.html](http://www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html); смотрите также Unsecured Economies Protecting Vital Information, McAfee, 2009, <http://resources.mcafee.com/content/NAUnsecuredEconomiesReport> [↑](#footnote-ref-58)
59. Robert Krysiak, "Semiconductor Mega-trends in 2010," *Forbes*, Jan. 2010, [www.forbes.com/2010/01/04/stmicroelectronics-healthcare-entertainment-technology-cio-network-semiconductors.html](http://www.forbes.com/2010/01/04/stmicroelectronics-healthcare-entertainment-technology-cio-network-semiconductors.html). [↑](#footnote-ref-59)
60. James Henry Carmouche, *IPsec Virtual Private Network Fundamentals*, Cisco Press, 19 July 2006, [www.ciscopress.com/bookstore/product.asp?isbn=1587052075](http://www.ciscopress.com/bookstore/product.asp?isbn=1587052075). [↑](#footnote-ref-60)
61. S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," The Internet Society, Dec. 1998, [www.ietf.org/rfc/rfc2460.txt](http://www.ietf.org/rfc/rfc2460.txt); Walter Goralski,, "The illustrated Network: How TCP/IP Works in a Modern Network", The Morgan Kaufmann Series in Networking, 2008, [www.freshwap.net/forums/e-books-tutorials/120250-illustrated-network-how-tcp-ip-works-modern-network.html](http://www.freshwap.net/forums/e-books-tutorials/120250-illustrated-network-how-tcp-ip-works-modern-network.html). [↑](#footnote-ref-61)
62. Hiroshi Ishii, "The tangible user interface and its evolution," *Communications of the ACM*, Vol. 51, Issue 6, June 2008, <http://portal.acm.org/citation.cfm?id=1349026.1349034>. [↑](#footnote-ref-62)
63. Steve Mann with Hal [Niedzviecki](http://www.amazon.com/s/ref=ntt_athr_dp_sr_2?_encoding=UTF8&sort=relevancerank&search-alias=books&field-author=Hal%20Niedzviecki), *Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer*, Doubleday of Canada, Nov. 2001. [↑](#footnote-ref-63)
64. *RFID* *Adoption and Implications*, European Commission (Enterprise & Industry Directorate-General, ICT for Competitiveness and Innovation), DG Enterprise & Industry, The Sectoral e-Business Watch, Impact Study No. 07/2008, Final Report, Sept. 2008, [www.ebusiness-watch.org/studies/special\_topics/2007/rfid.htm](http://www.ebusiness-watch.org/studies/special_topics/2007/rfid.htm);. Arun N. Nambiar, "RFID Technology: A Review of its Applications", Proceedings of the World Congress on Engineering and Computer Science 2009, Vol II, WCECS 2009, 20–22 October 2009, San Francisco, USA, [www.iaeng.org/publication/WCECS2009/WCECS2009\_pp1253-1259.pdf](http://www.iaeng.org/publication/WCECS2009/WCECS2009_pp1253-1259.pdf). [↑](#footnote-ref-64)
65. E. Aarts, R. Harwig, M. Schuurmans, chapter "Ambient Intelligence," in Peter J. Denning, ed., *The Invisible Future: The Seamless Integration Of Technology Into Everyday Life*, McGraw-Hill Companies, 2001 at 235-250; D. Wright, S. Gutwirth, M. Friedewald et al., *Safeguards in a World of Ambient Intelligence,* Springer, 2008,   
    [www.springer.com/computer/database+management  
    +&+information+retrieval/book/978-1-4020-6661-0](http://www.springer.com/computer/database+management+&+information+retrieval/book/978-1-4020-6661-0). [↑](#footnote-ref-65)
66. Vladimir Britkov, "Grid and Cloud Computing," Paper to the World Federation of Scientists Permanent Monitoring Panel on Information Security, May 2010 (далее "Britkov"). [↑](#footnote-ref-66)
67. Britkov. [↑](#footnote-ref-67)
68. Vladimir Britkov and Axel Lehmann, "Security challenges arising from innovations in information and communication technologies (ICT)," *International Seminar on Nuclear War and Planetary Emergencies*, 38th Session. E. Majorana Centre for Scientific Culture, Erice, Italy, 19-24 Aug. 2007 at 503515. [↑](#footnote-ref-68)
69. Kizito Ssamula Mukasa, Andreas Holzinger, Arthur I. Karshmer,"Intelligent User Interfaces for Ambient Assisted Living," Proceedings of the 13th International Conference on Intelligent User Interface, ISBN: 978-1-59593-987-6, 2008, <http://portal.acm.org/citation.cfm?id=1378856>; Fraunhofer IRB Verlag, ISBN 978-3-8167-7521-8, <http://verlag.fraunhofer.de/PDF/English_Publications_2010.pdf>. [↑](#footnote-ref-69)
70. P. [Rashidi,](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=Authors:.QT.Rashidi,%20P..QT.&newsearch=partialPref) D. J. [Cook](http://ieeexplore.ieee.org/search/searchresult.jsp?searchWithin=Authors:.QT.Cook,%20D.J..QT.&newsearch=partialPref),"Keeping the Resident in the Loop: Adapting the Smart Home to the User," in *Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions*, Sept. 2009, Vol. 39, [Issue:5](http://ieeexplore.ieee.org/xpl/tocresult.jsp?isnumber=5208652) at 949–959, <http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?reload=true&punumber=3468>; The CASAS Smart Home Project, Washington State University, USA, <http://ailab.eecs.wsu.edu/casas/>. [↑](#footnote-ref-70)
71. *Internet of Things* — An action plan for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, <http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf>; "Appendix F: The Internet of Things (Background), Disruptive Technologies: Global Trends 2025, SRI Consulting Business Intelligence, [www.dni.gov/nic/PDF\_GIF\_confreports/disruptivetech/  
    appendix\_F.pdf](http://www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf). [↑](#footnote-ref-71)
72. Mark Weiser, "[The Computer for the Twenty-First Century](http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html)," *Scientific American,* Sept.1991 at 94-110, www.cim.mcgill.ca/~jer/courses/hci/ref/weiser\_reprint.pdf. [↑](#footnote-ref-72)
73. McAfee Security Advice Center, <http://home.mcafee.com/advicecenter/>. [↑](#footnote-ref-73)
74. "Internet Security Threat Report,"Symantec, [www.symantec.com/business/theme.jsp?themeid  
    =threatreport](http://www.symantec.com/business/theme.jsp?themeid=threatreport). [↑](#footnote-ref-74)
75. Kaspersky, [www.kaspersky.co.uk/index.html](http://www.kaspersky.co.uk/index.html). [↑](#footnote-ref-75)
76. "Security Tech Center," <http://technet.microsoft.com/en-us/security/default.aspx>; SANS, www.sans.org/. [↑](#footnote-ref-76)
77. Определение и дальнейшее объяснение *смотрите*: <http://en.wikipedia.org/wiki/Malware>. [↑](#footnote-ref-77)
78. "The FORWARD Emerging ICT Threats Whitebook," [www.ict-forward.eu/whitebook/](http://www.ict-forward.eu/whitebook/). [↑](#footnote-ref-78)
79. Всемирная федерация ученых ранее рассматривала эту проблему при ее представлении Всемирной встрече на высшем уровне по вопросам информационного общества (ВВУИО) на Тунисской встрече 2005 года, "Information Security in the Context of the Digital Divide", а частности, в содержащейся в ней Рекомендации 5, "Denial of information access through Internet filtering", p. 12, and Explanatory Comments p. 2430, [www.itu.int/wsis/docs.2/tunis/contributions/co1,pdf](http://www.itu.int/wsis/docs.2/tunis/contributions/co1,pdf), , and [www.unbiw.de/infosecur](http://www.unbiw.de/infosecur). *Смотрите также*, с аналогичным посылом, как и в предыдущей главе, Henning Wegener "Cyber Repression: Framing the Problem. Assessing the State of Debate and Thinking of Counter-Strategies," in *Rights and Responsibilities in Cyberspace. Balancing the Need for Security and Liberty, 2010*, EastWest Institute and World Federation of Scientists, [www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty](http://www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty). [↑](#footnote-ref-79)
80. Index on Censorship is a prominent British organisation promoting freedom of expression, www.indexoncensorship.org. [↑](#footnote-ref-80)
81. Jo Glanville, "The big business of net censorship," *The Guardian*, 17 Nov. 2008, www.guardian.co.uk/commentisfree/2008/nov/17/censorship-internet. [↑](#footnote-ref-81)
82. OpenNet Initiative, [www.opennet.net](http://www.opennet.net). Проект использует международную сеть исследователей для определения масштаба и характера государственных программ фильтрации интернет. Участие научных учреждений включают Центр международных исследований в школа глобальной политики Муна Университете Торонто, Центр Berkman Интернет и общества в Гарвардской школе права, Оксфордский Институт интернет в Оксфордском университете, и группа SecDev, которая выросла из Исследовательской группы Advanced Network Кембриджской программы безопасности в Кембриджском университете. Смотрите также [www.chillingeffects.org](http://www.chillingeffects.org) с еще большей группой поддержки академических институтов, которые "мониторят правовой климат для интернет-активности." [↑](#footnote-ref-82)
83. Global Network Initiative, [www.globalnetworkinitiative.org](http://www.globalnetworkinitiative.org). [↑](#footnote-ref-83)
84. At least the IGF has shown that the censorship issue is not alien to the purview of its work. During the current debate on a continuation of the Forum’s work and a possible amplification of its mandate, proposals have been made for more dialogue on freedom of expression, and more attention to the development and human rights dimension of International Governance. *Смотрите* UN General Assembly document A/65/78 (E/2010/68) of 7 May 2010. [↑](#footnote-ref-84)
85. "Declaration on Fundamental Principles concerning the Contribution of the Mass Media to Strengthening Peace and International Understanding, to the Promotion of Human Rights and to Countering Racialism, Apartheid and Incitement to War," United Nations Educational, Scientific, and Cultural Organization, 28 Nov. 1978, [http://portal.unesco.org/en/ev.php-URL\_ID=  
    13176&URL\_DO=DO\_PRINTPAGE&URL\_SECTION=201.html](http://portal.unesco.org/en/ev.php-URL_ID=13176&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html); "Recommendations concerning the Promotion of Use of Multilingualism and Universal Access to Cyberspace," United Nations Educational, Scientific, and Cultural Organization, 15 Oct. 2003, <http://portal.unesco.org/ci/en/ev.php-URL_ID=13475&URL_DO=DO_TOPIC&URL_SECTION=201.html> (advocating "universal access to the Internet as an instrument for promoting the realization of the human rights as defined in Art. 19 and 27 of the Universal Declaration of Human Rights"). [↑](#footnote-ref-85)
86. Global Cyber Risk, LLC; Washington, DC, USA. [↑](#footnote-ref-86)
87. Massachusetts Institute of Technology, Cambridge, MA, USA. [↑](#footnote-ref-87)
88. Institute for Systems Analysis, Russian Academy of Sciences, Moscow, Russia. [↑](#footnote-ref-88)
89. Например, "The mission of the United States Air Force is to deliver sovereign options for the defense of the United States of America and its global interests—to fly, fight, and win in Air, Space, and Cyberspace." "Air Force Strategy: Sovereign Options for Securing Global Stability and Prosperity," 26 Mar. 2008, Office of the Secretary of the Air Force, [www.stormingmedia.us/  
    98/9868/A986884.html](http://www.stormingmedia.us/98/9868/A986884.html). The US perspective is further elaborated in *Information Operations, Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service (CRS) Report, RL31787, 14 Sept. 2006, [www.fas.org/irp/crs/RL31787.pdf](http://www.fas.org/irp/crs/RL31787.pdf) (далее "CRS Report"). [↑](#footnote-ref-89)
90. Gen. John Casciano, "Threat Considerations and the Law of Armed Conflict," Aug. 2005 (on file with WFS Information Security PMP). [↑](#footnote-ref-90)
91. Об атаке широко сообщалось в международной прессе. Например, смотрите*,* Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian,* 17 May 2007, www.guardian.co.uk/world/2007/may/17/topstories3.russia. [↑](#footnote-ref-91)
92. By early June a leader of the pro-Putin Russian youth group, Nashi, had claimed credit for the attack. [www.rferl.org/content/Russian\_Groups\_Claims\_Reopen\_Debate\_On\_Estonian\_Cyberattacks\_/  
    1564694.html](http://www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html) . The veracity of the claim is unknown. [↑](#footnote-ref-92)
93. *Tracking GhostNet: Investigation of a Cyber Espionage Network,* Information Warfare Monitor, 1 Sept. 2009, [www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/](http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/). "Расследование, в конечном итоге, обнаружило сеть из более 1295 зараженных хостов в 103 странах. До 30% от зараженных хостов были дорогостоящими целями и включали компьютеры, расположенные в министерствах иностранных дел, посольствах, международных организациях, СМИ и НПО. Компьютерную систему Тибета мы исследовали вручную, с нее начались наши исследования, она была окончательно скомпрометирована посредством нескольких заражений, которые дали нападавших беспрецедентный доступ к потенциально чувствительной информации .... Но приписывать все китайские вредоносные программы конкретному или целевому сбору разведывательных данных, осуществляемому Китайским государством, является неправильным и вводит в заблуждение. Числа могут рассказать другую историю. Население Китая в настоящее время пользователь интернет в мире. Огромное количество молодых "digital native" в онлайновом режиме может более чем просто увеличить число китайских вредоносных программ. Поскольку компьютеры используют все более творческие люди, ожидается, что Китай (и китайские физические лица) составит большую часть киберпреступности." [↑](#footnote-ref-93)
94. Ariana Eunjung Cha and Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say," *The Washington Post*, 14 Jan. 2010, [www.washingtonpost.com/wp-dyn/content/  
    article/2010/01/13/AR2010011300359.html](http://www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html). [↑](#footnote-ref-94)
95. Например, в 2009 году бывший директор Национальной разведки США Майк МасКоннел (Mike McConnell) определил кибероружие как оружие массового разрушения, или имеющее такую возможность. CRS Report at 3. [↑](#footnote-ref-95)
96. "ENISA commenting on massive cyber attacks in Estonia," ENISA press release, 24 May 2007, [www.enisa.europa.eu/act/cert/contact/press-releases/enisa-commenting-on-massive-cyber-attacks-in-estonia](http://www.enisa.europa.eu/act/cert/contact/press-releases/enisa-commenting-on-massive-cyber-attacks-in-estonia). [↑](#footnote-ref-96)
97. Bonnie N. Adkins, "The Spectrum Of Cyber Conflict: From Hacking to Information Warfare: What Is Law Enforcement’s Role?" Air Command and Staff College, Maxwell Air Force Base, AU/ACSC/003/2001-04, Apr. 2001, [http://stinet.dtic.mil/oai/oai?&verb=getRecord&  
    metadataPrefix=html&identifier=ADA406949](http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA406949). [↑](#footnote-ref-97)
98. Например, "Любая функция, устройство или сочетание возможностей и методов, которые, при их использовании по прямому назначению, могла бы нарушить целостность и доступность данных, программ или информации, находящейся в компьютере или системы обработки информации." Graham H. Todd, "Armed Attack In Cyberspace: Deterring Asymmetric Warfare With An Asymmetric Definition," *Air Force Law Review,* Vol. 64, 2009 at 65 – 102, [http://lawlib.wlu.edu/CLJC/  
    index.aspx?mainid=418&issuedate=2010-03-23&homepage=no](http://lawlib.wlu.edu/CLJC/index.aspx?mainid=418&issuedate=2010-03-23&homepage=no). [↑](#footnote-ref-98)
99. Решение военного ведомства США не проводить кибератаки на финансовые системы Ирака обсуждалось в *Information Warfare and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service, RL31787, 19 July 2004 at 5-6, [www.fas.org/irp/crs/RL31787.pdf](http://www.fas.org/irp/crs/RL31787.pdf). Этот отчет CRS также создал структуру военного ведомства США по вопросам кибервойн, и в нем объясняется, когда можно применять кибервойны в рамках долгосрочной военной стратегии и программ информационной войны. [↑](#footnote-ref-99)
100. Хактивизмом называют написание или использование компьютерных программ (хакерство) для атаки ИКТ сетей жертвы с целью продвижения политической идеологии или общественной цели. Хактивисты часто определяют свои действия как акты протеста и гражданского неповиновения. Например, *смотрите* <http://thehacktivist.com/hacktivism.php>. [↑](#footnote-ref-100)
101. Clive Walker, "Cyber-Terrorism: Legal Principle and the Law in the United Kingdom," *Penn State Law Review,* Vol. 110, 2006 at 625-65, [http://papers.ssrn.com/sol3/papers.cfm?abstract\_id  
     =1109113#%23](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109113#%23). [↑](#footnote-ref-101)
102. По законам США средства доставки подозреваемого на территориальную юрисдикцию не являются юрисдикционной защитой от судебного преследования. [↑](#footnote-ref-102)
103. Смотрите статью "Концепция кибермира" Хэннинга Вегенера в этой книге. [↑](#footnote-ref-103)
104. Впервые представлено на конференции ANSER Института безопасности Отечества "Homeland Security 2005: Charting the Path Ahead", Университет Мэриленд, презентация Джоди Вестбай "A Shift in Geo-Cyber Stability and Security", 6–7 мая 2002 года. [↑](#footnote-ref-104)
105. Хартия ООН, www.un.org/en/documents/charter/index.shtml. [↑](#footnote-ref-105)
106. Североатлантический договор, [www.nato.int/cps/en/natolive/official\_texts\_17120.htm](http://www.nato.int/cps/en/natolive/official_texts_17120.htm). [↑](#footnote-ref-106)
107. Женевская конвенция 1949 года, [www.icrc.org/web/eng/siteeng0.nsf/html/genevaconventions](http://www.icrc.org/web/eng/siteeng0.nsf/html/genevaconventions). [↑](#footnote-ref-107)
108. Женевский Дополнительный протокол к Женевской конвенции от 12 августа 1949 года, касающийся защиты жертв вооруженных международных конфликтов (Протокол I), 8 июня 1977 года,   
     [www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e  
     0052b079](http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079) ("далее Protocol I"). [↑](#footnote-ref-108)
109. Конвенции о законах и обычаях сухопутной войны (Гаага II), 29 июля 1899 г., <http://avalon.law.yale.edu/19th_century/hague02.asp>; Законы и обычаи сухопутной войны (Гаага IV), 18 октября 1907 г., <http://avalon.law.yale.edu/20th_century/hague04.asp>. [↑](#footnote-ref-109)
110. Конвенции о запрещении или ограничении применения определенных видов обычного вооружения, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие, 28 ноября. 2003 г., [www.icrc.org/web/eng/siteeng0.nsf/html/p0811](http://www.icrc.org/web/eng/siteeng0.nsf/html/p0811) (далее "Convention on Weapons Excessively Injurious"). [↑](#footnote-ref-110)
111. *Смотрите* Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace,* Aegis Research Corp., Falls Church, VA, 2000; *The Law of Armed Conflict: Basic Knowledge,* International Committee of the Red Cross, June 2002, [www.icrc.org](http://www.icrc.org). [↑](#footnote-ref-111)
112. *The Insider Threat to U.S. Government Information Systems*, National Security Telecommunications and Information Systems Security Committee, NSTISSAM INFOSEC/1-99, [www.cnss.gov/Assets/pdf/  
     nstissam\_infosec\_1-99.pdf](http://www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf). [↑](#footnote-ref-112)
113. Более подробное обсуждение эстонского и грузинского конфликтов, реагирования и юридических проблем описано в материалеJody R. Westby, "The Path to Cyber Stability," *Rights and Responsibiliites in Cyberspace: Balancing the Need for Security and Liberty",* EastWest Institute and World Federation of Scientists, 2010 at 1, [www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty](http://www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty). [↑](#footnote-ref-113)
114. *Смотрите*, например, "Protection of civilian persons and populations in time of war," extract from "Basic rules of the Geneva Convention and their Additional Protocols", International Committee of the Red Cross, 31 Dec. 1988, [www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV](http://www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV) (далее "Protection of civilian persons") ("экстраординарные разработки в области воздушной войны привели к необходимости разработки и конкретизации существующих законов вооруженных конфликтов. Это является предметом Части IV или Первого Дополнительного протокола к Конвенции."); Женевская конвенция II была добавлена для учета использования в войне военно-морских флотов и решения вопроса о лечении раненых, больных, потерпевших кораблекрушение и военнослужащих на море. [↑](#footnote-ref-114)
115. "Protection of civilian persons and populations in time of war", extract from "Basic rules of the Geneva Convention and their Additional Protocol", International Committee of the Red Cross, 31 Dec. 1988, [www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV](http://www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV). [↑](#footnote-ref-115)
116. Declaration, Prohibiting Launching of Projectiles and Explosives from Balloons (Hague, IV); 29 July 1899, <http://avalon.law.yale.edu/19th_century/hague994.asp>. [↑](#footnote-ref-116)
117. Declaration on the Use of Projectiles the Object of Which is the Diffusion of Asphyxiating or Deleterious Gases, The Hague Conference of 1899, 29 July 1899, <http://avalon.law.yale.edu/19th_century/dec99-02.asp>. [↑](#footnote-ref-117)
118. Declaration on the Use of Bullets Which Expand or Flatten Easily in the Human Body, The Hague Conference, 29 July 1899, <http://avalon.law.yale.edu/19th_century/dec99-03.asp>. [↑](#footnote-ref-118)
119. Convention on Weapons Excessively Injurious. [↑](#footnote-ref-119)
120. Смотрите различные ссылки в "публикациях" и "действиях" на сайте [www.unibw.de/infosecur](http://www.unibw.de/infosecur), и, в особенности, стенограмму конференции в декабре 2008 года "The Global Internet Crisis: The Quest for Cyber Peace". [↑](#footnote-ref-120)
121. "UN Chief proposes int’l accord to prevent cyber war," 31 Jan. 2010, [www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a](http://www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a). [↑](#footnote-ref-121)
122. The Susan Mbarek Women’s International Peace Movement, The Cyber Peace Initiative, [http://smwipm.cyber peaceinitiative.org/](http://smwipm.cyberpeaceinitiative.org/). [↑](#footnote-ref-122)
123. "A Declaration on A Culture of Peace," UNESCO, A/Res/53/243, [www.unesco.org/  
     cpp/uk/declarations/2000.htm](http://www.unesco.org/cpp/uk/declarations/2000.htm). [↑](#footnote-ref-123)
124. "Erice Declaration on Principles for Cyber Stability and Cyber Peace," World Federation of Scientists, Aug. 2009, [www.ewi.info/system/files/**Erice**.pdf](http://www.ewi.info/system/files/Erice.pdf). [↑](#footnote-ref-124)
125. *Смотрите Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Report and Recommendations, World Federation of Scientists Permanent Monitoring Panel on Information Security, Nov. 19, 2003, Submission to the World Summit on the Information Society, [www.itu.int/dms\_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf](http://www.itu.int/dms_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf). [↑](#footnote-ref-125)
126. *Смотрите* Sergei Komov, Sergei Korotkov, Igor Dylewski, "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law," *ICTs and International Security*, United Nations Institute for Disarmament Research, 2007, [www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/  
     ?fecvnodeid=128420&dom=1&groupot593=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&fecvid=21&ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&v21=128420&lng=en&id=47166](http://www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?fecvnodeid=128420&dom=1&groupot593=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&fecvid=21&ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&v21=128420&lng=en&id=47166). [↑](#footnote-ref-126)
127. Смотрите, например, Martin C. Libicki "Cyber deterrence and Cyberwar", Santa Monica, 2009, p. 158 et. seq. [↑](#footnote-ref-127)
128. Смотрите ГлавуVII. [↑](#footnote-ref-128)
129. "Международное сообщество должно знать, что небольшая киберстычка может быть предвестником большого киберконфликта, который способен разжечь региональные физические действия, которые будут иметь международные последствия". Цитата из John Bumgarner, Chief Technology Officer, US Cyber Consequences Unit, *Jane’s Defence Weekly*, 29 Sept. 2010, [www.jdw.janes.com](http://www.jdw.janes.com) (далее "Jane’s"). [↑](#footnote-ref-129)
130. В момент написания этого документа страны НАТО в ходе подготовки к саммиту государств  участников Вашингтонского договора (20 ноября 2010 г.) рассматривали коллективные решения относительно новых угроз, включая кибератаки. Следует ли относить такие атаки вызывать действия по коллективной обороне, Статья. 4 (взаимные консультации) и Статья 5 (взаимопомощь с принятием таких мер, которые "считаются необходимыми, включая применение вооруженной силы"). [↑](#footnote-ref-130)
131. "Клаусвитц (Clausewitz) не мог предвидеть, что наилучшей защитой в XXi-м веке будет сильная киберзащита." Jane’s. [↑](#footnote-ref-131)
132. Например, Южная Африка только недавно (февраль 2010 г.) объявил о своем намерении приступить к разработке национальной скоординированной политики кибербезопасности. "Notice of Intention to Make South African Cybersecurity Policy," Republic of South Africa, Government Gazette, No. 32963, 19 Feb. 2010, [www.pmg.org.za/files/docs/100219cybersecurity.pdf](http://www.pmg.org.za/files/docs/100219cybersecurity.pdf). [↑](#footnote-ref-132)
133. "Cyberwar: Sabotaging the System – 60 Minutes – CBS News," 8 Nov. 2009, [www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml](http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml) (reporting that the U.S. Congress has allocated USD 17 billion for cybersecurity offensive and defensive initiatives). [↑](#footnote-ref-133)
134. David Eshel, "Israel Adds Cyber-Attack to IDF," *Military.com,* 10 Feb. 2010, [www.military.com/features/0,15240,210486,00.html](http://www.military.com/features/0,15240,210486,00.html) (далее "Eshel"). [↑](#footnote-ref-134)
135. Kevin Coleman, "Russia’s Cyber Forces," DefenseTech, 27 May 2008, <http://defensetech.org/2008/05/27/russias-cyber-forces/>. [↑](#footnote-ref-135)
136. Gregory Asmolov, "Russia: New Military Doctrine and Information Security," Global Voices, 23 Feb. 2010, <http://globalvoicesonline.org/2010/02/23/russian-military-doctrine/> (describing Russia’s updated military doctrine, which classifies information warfare as a form of military aggression). [↑](#footnote-ref-136)
137. *Смотрите, например*, Jo Biddle, "AFP: Huge leak of secret files sows new Afghan war doubts," 27 July 2010, [www.google.com/hostednews/afp/article/ALeqM5gZkjOIqwM0xJDr0u5fPrc5rxdEQg](http://www.google.com/hostednews/afp/article/ALeqM5gZkjOIqwM0xJDr0u5fPrc5rxdEQg). [↑](#footnote-ref-137)
138. *Cyberwarfare*, Congressional Research Service, RL30735, Updated 19 June 2001, [www.fas.org/irp/crs/RL30735.pdf](http://www.fas.org/irp/crs/RL30735.pdf) (цитируети русского военного чиновника, который исключил возможность описания информационной войны как невоенной) (далее "CRS Кибервойны"). *Смотрите также* Peter Beaumont, "US appoints first cyberwarfare general," Guardian.co.uk, 23 May 2010, [www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general/](http://www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general/) (reporting that the United States has also indicated it might consider using conventional military tactics to respond to cyber attacks) (далее "Cyber General"). [↑](#footnote-ref-138)
139. President Barack Obama, "Remarks by the President on Securing Our Nation’s Cyber Infrastructure," The White House, 29 May 2009, [www.whitehouse.gov/the\_press\_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure](http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure) (сообщает, что цифровая инфраструктура страны теперь будет рассматриваться как "стратегический национальный актив", и что ее защита будет "приоритетом национальной безопасности"). [↑](#footnote-ref-139)
140. Iran (estimating Iran’s кибервойны budget at around USD 76 million). [↑](#footnote-ref-140)
141. Gurmeet Kanwal, "China’s Emerging Cyber War Doctrine," at 20, Journal of Defense Studies, 2009, available at: www.idsa.in/system/files/jds\_3\_3\_gkanwal\_0.pdf (discussing China’s Information Warfare and Acupuncture policy). [Далее "Kanwal"] [↑](#footnote-ref-141)
142. Кибервойны: An Analysis of the Means and Motivations of Selected Nation States, Dartmouth College, Institute for Security, Technology, and Society, Nov. 2004 at 2, [www.ists.dartmouth.edu/docs/execsum.pdf](http://www.ists.dartmouth.edu/docs/execsum.pdf) (далее "Selected Nations"). [↑](#footnote-ref-142)
143. *See, e.g.,* Richard Westcott, "UK Seeks Next Generation of Cybersecurity Specialists," *BBC News*, 26 July 2010, [www.bbc.co.uk/news/technology-10742588](http://www.bbc.co.uk/news/technology-10742588). [↑](#footnote-ref-143)
144. Kanwal at 20. [↑](#footnote-ref-144)
145. Gordon Corera, "Cyber-security strategy launched," *BBC News,* 25 June 2009, <http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm?ad=1> (далее "Corera"); Tom Gjelten, "Cyberwarrior Shortage Threatens U.S. Security," National Public Radio, 19 July 2010, [www.npr.org/templates/story/story.php?storyId=128574055](http://www.npr.org/templates/story/story.php?storyId=128574055). [↑](#footnote-ref-145)
146. Eshel. [↑](#footnote-ref-146)
147. Kanwal at 20. [↑](#footnote-ref-147)
148. Некоторые страны раскрыли свои многочисленые перемены персонала. Смотрите Cyber General (сообщает, что США объявили о переквалификациии 30 000 военнослужащих на кибервойны). Однако информация о статегиях многих стран менее доступна. Смотрите Robert McMillan, "Black Hat Talk on China’s ‘Cyber Army’ Pulled After Pressure", *InfoWorld*, 15 July 2010, www.infoworld.com/print/130362. [↑](#footnote-ref-148)
149. Eshel*.* [↑](#footnote-ref-149)
150. Например, США в 2009 году объявили о создании нового кибервоенного департамента. Cyber General. Соединенное Королевство также недавно объявило о создании центра кибервоенных операций в составе своей стратегии кибербезопасности. Corera. [↑](#footnote-ref-150)
151. *Смотрите* "U.S. Cyber Command Fact Sheet," U.S. Department of Defense, 25 May 2010, [www.defense.gov/home/features/2010/0410\_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf](http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf) [↑](#footnote-ref-151)
152. Siobhan Gorman, "U.S. Backs Talks on Cyberwarfare," *The Wall Street Journal*, 4 June 2010, <http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html> (noting that 90 per cent of U.S. military power is provided by the private sector, according to U.S. military officials) (далее "Gorman"). [↑](#footnote-ref-152)
153. Kanwal at 16. [↑](#footnote-ref-153)
154. Kanwal at 14. [↑](#footnote-ref-154)
155. Kanwal at 18. [↑](#footnote-ref-155)
156. Radical Change("Because the United States is the most Internet-dependent and automated. it’s also the most vulnerable to cyberattack."). [↑](#footnote-ref-156)
157. Kanwal at 18; CRS Кибервойны at 11. [↑](#footnote-ref-157)
158. *Смотрите, например,* Selected Nations at 5 (recommending systematic and sustained efforts to change the way the U.S. populace views network security in order to improve national cybersecurity). [↑](#footnote-ref-158)
159. Например, Mauritius’ National Computer Board, under the purview of its Ministry of Information and Communication Technology, oversees a Cybersecurity Awareness Portal, available at: [www.gov.mu/portal/sites/ncbnew/main.jsp](http://www.gov.mu/portal/sites/ncbnew/main.jsp), а США каждый октябрь проводит Национальный месяц знаний о кибербезопасности. Частно-государственные партнерства типа Национальный альянс США по кибербезопасности, также информирует пользователей и руководителей цифровой инфрастурктуры о том, как создавать устойчивые системы и механизмы защиты. *Смотрите* "About Us," The National Cybersecurity Alliance, [www.staysafeonline.org/content/about-us](http://www.staysafeonline.org/content/about-us). [↑](#footnote-ref-159)
160. *See, e.g.*, Understanding at 20 (перечисляет основные цели различных хакерских атак, включая Пентагон, Правительство Германии, Google, Ebay и NASA). [↑](#footnote-ref-160)
161. *Смотрите id.* at 23–24. [↑](#footnote-ref-161)
162. Например, взлом Центрального командования США в 2008 году был осуществлен посредством инфицированных флеш-драйверов. *Смотрите* Fifth Domain. [↑](#footnote-ref-162)
163. Martyn Williams, "North Korea Moves Quietly Onto the Internet," *Computerworld*, 10 June 2010, www.computerworld.com/s/article/9177968/North\_Korea\_moves\_quietly\_onto\_the\_Internet. [↑](#footnote-ref-163)
164. Corera*.* [↑](#footnote-ref-164)
165. *Смотрите, например*, "Economic and Social Council Opens General Segment of 2010 Session," at 3, ECOSOC/6444, 16 July 2010, www.un.org/News/Press/docs/2010/ecosoc6444.doc.htm (обсуждение "киберденег" или системы электронных денег, используемой в Африканских странах) (далее "ECOSOC 2010"). [↑](#footnote-ref-165)
166. Gorman. [↑](#footnote-ref-166)
167. "Draft Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World," Declaration 42, Twelfth United Nations Congress on Crime Prevention and Criminal Justice, 18 Apr. 2010, [www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/  
     ACONF.213L6\_Rev.2/V10529031A\_CONF213\_L6\_REV2\_E.pdf](http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529031A_CONF213_L6_REV2_E.pdf). [↑](#footnote-ref-167)
168. "Report of the Twelfth United Nations Congress on Crime Prevention and Criminal justice", UNODC, Salvador, Brazil, 12–19 Apr. 2010, [www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A\_CONF.213\_18/V1053828e.pdf](http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf) [↑](#footnote-ref-168)
169. "Summary of outcome regarding cybercrime: 12th UN Congress on Crime Prevention and Criminal Justice," Project on Cybercrime, 26 Apr. 2010, http://www.coe.int/t/dghl/cooperation/  
     economiccrime/cybercrime/2079\_UNCC\_cyberoutcome.pdf. [↑](#footnote-ref-169)
170. ECOSOC 2010. [↑](#footnote-ref-170)
171. *Id.* (discussing the "digital cash" or electronic money system used in African countries). [↑](#footnote-ref-171)
172. "Defending Against Cyber Attacks," NATO, [www.nato.int/cps/en/natolive/topics\_49193.htm](http://www.nato.int/cps/en/natolive/topics_49193.htm). [↑](#footnote-ref-172)
173. "NATO 2020", www.nato.int/cps/en/natolive/official\_texts\_63654.htm?selectedLocale=en. [↑](#footnote-ref-173)
174. Cooperative Cyber Defense Center for Excellence, www.ccdcoe.org/. [↑](#footnote-ref-174)
175. "Defence exercise to boost skills for countering cyber attacks," NATO-News, 10 May 2010, www.nato.int/cps/en/SID-012B6A76-D60B9579/natolive/news\_63177.htm. [↑](#footnote-ref-175)
176. "NATO and Estonia conclude agreement on cyber defense," NATO-News, 23 Apr. 2010, www.nato.int/cps/en/natolive/news\_62894.htm. [↑](#footnote-ref-176)
177. Convention on Cybercrime CETS no.: 185, Council of Europe, <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG> (last visited on 10 Aug. 2010 (далее "Convention"). [↑](#footnote-ref-177)
178. "National Security Threats in Cyberspace," American Bar Association, Standing Committee on Law and National Security and National Strategy Forum, Sept. 2009 at 13, [www.abanet.org/natsecurity/threats\_%20in\_cyberspace.pdf](http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf) (далее "Workshop"). [↑](#footnote-ref-178)
179. Convention. [↑](#footnote-ref-179)
180. "Bilateral Cooperation: Asia," India Department of Information Technology, Government of India Ministry of Communications and IT, [www.mit.gov.in/content/bilateral-cooperation](http://www.mit.gov.in/content/bilateral-cooperation) (далее "Cooperation"). [↑](#footnote-ref-180)
181. Например, сотрудничество Индии с Брунеем, Малайзией, Францией и Авсралией, в частности, сфокусирвоанное н информационной безопасности и/или киберпреступности, тогда как другие типы взаимодействия концентрируются на разработке ресурсов и устройств Cooperation. [↑](#footnote-ref-181)
182. "Malaysia and Morocco Are Now Partners in Cybersecurity," CyberSecurity Malaysia, 24 Jan. 2010, www.cybersecurity.my/data/content\_files/44/632.pdf?.diff=1265036362. [↑](#footnote-ref-182)
183. Для получения полной информации об этой оперативной группе, посетите сайт www.itu.int/  
     ITU-T/focusgroups/smart/. [↑](#footnote-ref-183)
184. Оперативные группы МСЭ-T, доступно по адресу: www.itu.int/ITU-T/focusgroups/. [↑](#footnote-ref-184)
185. Сведения об оперативной группе МСЭ-T по "умным" электросетям доступны по адресу: www.itu.int/ITU-T/focusgroups/smart/tor.html. [↑](#footnote-ref-185)
186. Радикальные изменения (цитирование бывшего советника президента США по безопасности Ричарда Кларка, утверждающего, что "сила, которая предотвратила ядерную войну – устрашение – неэффективно в кибервойнах"). [↑](#footnote-ref-186)
187. Tang Lan and Zhang Xin, "Can Cyber Deterrence Work?" in *Global Cyber Deterrence: Views from China, The U.S., Russia, India, and Norway,* EastWest Institute, Apr. 2010 at 1, www.ewi.info/system/files/CyberDeterrenceWeb.pdf. [↑](#footnote-ref-187)
188. James A Lewis*,* "Cross-Domain Deterrence and Credible Threats," Center for Strategic and International Studies, July 2010, <http://csis.org/files/publication/100701Cross_Domain_Deterrence.pdf>. [↑](#footnote-ref-188)
189. *Id*. [↑](#footnote-ref-189)
190. *Id.* [↑](#footnote-ref-190)
191. Workshop at 14. [↑](#footnote-ref-191)
192. *Id.* [↑](#footnote-ref-192)
193. *Id.* [↑](#footnote-ref-193)
194. "ВВУИО: Тунисская программа для информационного общества." Пункт 40, Всемирная встреча на высшем уровне по вопросам информационного общества, WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 Nov. 2005, [www.itu.int/wsis/docs2/tunis/off/6rev1.html](http://www.itu.int/wsis/docs2/tunis/off/6rev1.html) (далее "Tunis Agenda"). [↑](#footnote-ref-194)
195. Участники семинара, включая членов Американского комитета законности и национальной безопасности, Фонда МакГормика (McCormick Foundation) и Форума по национальной стратегии, поддержали создание Международной целевой группы по кибербезопасности для разраотки кибернорм и правил для улучшения кибербезопасности. Workshop at 26. [↑](#footnote-ref-195)
196. Robert Mullins, "‘Pearl Harbor’ post struck a nerve," *NetworkWorld*, 11 Mar. 2010, [www.networkworld.com/community/node/58450](http://www.networkworld.com/community/node/58450) (цитирует бывшего советника по безопасности Президента США Ричарда Кларка (Richard Clarke) на недавней дискусии комитета по кибербезопасности). [↑](#footnote-ref-196)
197. Convention Against Transnational Organized Crime, United Nations Office on Drugs and Crime, 2004, www.unodc.org/unodc/en/treaties/CTOC/index.html. [↑](#footnote-ref-197)
198. Universal Declaration of Human Rights, Article 19, U.N. G.A., Res. 217A (III), U.N. GAOR, U.N. Doc. A/810, 1948, www.un.org/en/documents/udhr/index.shtml#a19. [↑](#footnote-ref-198)
199. Geneva Declaration of Principles, Para. 4, World Summit on the Information Society, 2003,: www.itu.int/dms\_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf. [↑](#footnote-ref-199)
200. "Ban urges greater use of digital technology to improve living conditions," UN News Centre, 17 May 2010, www.un.org/apps/news/story.asp?NewsID=34716. [↑](#footnote-ref-200)
201. National Statement of the United States, 2010 Nuclear Security Summit, 13 Apr. 2010, [www.whitehouse.gov/the-press-office/nuclear-security-summit-national-statement-united-states](http://www.whitehouse.gov/the-press-office/nuclear-security-summit-national-statement-united-states) (hereinafter "National Statement of the United States"). [↑](#footnote-ref-201)
202. *Id.* [↑](#footnote-ref-202)
203. Treaty on the Non-Proliferation of Nuclear Weapons (NPT), Art. 3, 1970, [www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglish\_Text.pdf](http://www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglish_Text.pdf) (далее "NPT"). [↑](#footnote-ref-203)
204. National Statement of the United States. [↑](#footnote-ref-204)
205. NPT at Preamble and Art. 5. [↑](#footnote-ref-205)
206. *Id.* at Preamble. [↑](#footnote-ref-206)
207. *Id.* at Art. 3. [↑](#footnote-ref-207)
208. *Id.* [↑](#footnote-ref-208)
209. "The Global Initiative to Combat Nuclear Terrorism", U.S. Dept. of State, www.state.gov/t/isn/c18406.htm. [↑](#footnote-ref-209)
210. "Statement of Principles", The Global Initiative to Combat Nuclear Terrorism, US Dept. of State, www.state.gov/documents/organization/141995.pdf. [↑](#footnote-ref-210)
211. Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (the "Outer Space Treaty"), Principle 6, 1967, www.oosa.unvienna.org/oosa/SpaceLaw/  
     lpos.html. [↑](#footnote-ref-211)
212. "Регламент международной электросвязи: Заключительные акты Всемирной административной конференции по телеграфии и телефонии", Международный союз электросвязи, 1988 год, www.itu.int/osg/spu/intset/itu-t/mel88/mel-88-e.pdf. [↑](#footnote-ref-212)
213. Тунисская программа. [↑](#footnote-ref-213)
214. "Международное многостороннее партнерство против киберугроз", Международный союз электросвязи, [www.itu.int/ITU-D/cyb/cybersecurity/impact.html](http://www.itu.int/ITU-D/cyb/cybersecurity/impact.html). [↑](#footnote-ref-214)
215. Информационное письмо МСЭ, разосланное всем государствам-членам ["Deployment of Cybersecurity Capabilities - IMPACT Global Response Centre"](%20“Deployment%20of%20Cybersecurity%20Capabilities%20-%20IMPACT%20Global%20Response%20Centre”), www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter-sent-to-member-states-2009.pdf. [↑](#footnote-ref-215)