网络犯罪

了解网络犯罪：现象、挑战及法律对策

报告

电信发展部门

了解网络犯罪：
现象、挑战及法律对策

2014 年 11 月

国际电联出版物《了解网络犯罪：现象、挑战及法律对策》由Marco Gercke博士教授起草。作者谨向国际电联电信发展局基础设施、环境建设和电子应用部致谢。

本出版物可在以下网址在线提供：www.itu.int/ITU-D/cyb/cybersecurity/legislation.html

打印本报告前请对环境有所考虑。

目录

目的

国际电联报告《了解网络犯罪：现象、挑战及法律对策》（以下简称《报告》）旨在帮助各国了解网络犯罪和网络安全方面的法律问题，并帮助协调法律框架。同样，《报告》旨在帮助各国更好地了解有关日益增长之网络威胁在国家和国际层面的含义，评估现有国家、区域和国际层面机制的需求，帮助各国建立良好的法律基础。

本《报告》全面论述了与网络犯罪法律方面问题最为相关的各主题，同时着重于考虑发展中国家的需求。由于网络犯罪的跨国特性，发展中国家和发达国家的法律文件是相同的。但在选择使用的参考文献时，除提供宽泛的资源选择范围、以更加深入地对不同的主题开展研究之外，还注重考虑到发展中国家的利益。在可能的情况下，采用的均为公开提供的来源，包括许多免费的在线法律期刊。

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

本出版物论述国际电联《全球网络安全议程》（GCA）七个战略目标中的第一个目标，它呼吁精心安排有关制定网络犯罪法律的战略，使之全球适用、可实现与现有国家和区域法律体系的互操作；《报告》还论述了按照 ITU-D 第 1 研究组第 22/1 号课题进行的、组织国家网络安全工作的方法。建立适当的法律基础设施是国家网络安全战略的一个有机组成部分。国际电联全权代表大会第 130 号决议（2010 年，瓜达拉哈拉，修订版） – 加强国际电联在树立使用信息通信技术的信心和提交安全性方面的作用 – 强调了国际电联在能力建设方面的职责。所有国家都采用适当的法律，以防 ICT 误用于犯罪或其他目的，包括旨在影响国家关键信息基础设施完整的活动，是实现全球网络安全的核心。由于网络威胁可来自全球的任何地方，因此面临的挑战本质上是面向国际范围的，为此需要国际合作、调查援助以及共同的实体法规和程序法规。因此，重要的是，各国之间协调好其法律框架，以便与网络犯罪作斗争，促进国际合作。

有关超级链接的免责声明

本文件包含指向公开可用文件的几百条超级链接。在将这些链接加入到本文件的脚注时已对所有参考文献均进行了检查。但不能保证链接所指网页的最新内容依然保持不变。为此，参考文献亦尽可能包含了相关出版物的作者或出版机构的信息、其标题及出版年份（可能的情况下），以方便读者在链接所指文件不再可用的情况下搜索该文件。

1. 引言

参考书目（节选）： *Aggarwal,* Role of e-Learning in A Developing Country Like India, Proceedings of the 3rd National Conference, INDIA, Com 2009*; Barney*, Prometheus Wired: The Hope for Democracy in the Age of Network Technology, 2001; *Choudhari/Banwet/Gupta*, Identifying Risk Factors in for E-governance Projects, published in Wgarwal/Ramana, Foundations of E-government, 2007, page 270 *et. seq.*; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006; *Dutta/De Meyer/Jain/Richter*, The Information Society in an Enlarged Europe, 2006; *Ekundayo/Ekundayo*, Capacity constraints in developing countries: a need for more e-learning space? The case of Nigeria, Proceedings ascilite Auckland, 2009, page 243 *et seq.*; *European Commission,* Final Report on Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure, 2009; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141 *et seq.*; *Gercke*, Cybersecurity Strategy, Computer Law Review International 2013, 136 *et seq.; Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2; *Masuda*, The Information Society as Post-Industrial Society, 1980; *Molla*, The Impact of eReadingness on eCommerce Success in Developing Countries, 2004; *Ndou*, E-Government for Developing Countries, Opportunities and Challenges, DJISDC 2004, 18, page 1 *et seq.*; *Luiijf/Klaver*, In Bits and Pieces, Vulnerability of the Netherlands ICT-infrastructure and consequences for the information society, 2000; *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, 2005; *Tanebaum*, Computer Networks, 2002; *Wigert*, Varying policy responses to Critical Information Infrastructure Protection (CIIP) in selected countries, Cybercrime and Security, IIB-1; *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, page 52-56; *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2.

1.1 基础设施与服务

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

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

信息通信技术对社会的影响远远超过建立基本的信息基础设施。信息通信技术的可用性是在创建、提供和使用基于网络之服务的发展过程中的基础，[8] 电子邮件已经取代了传统的信件；[9] 如今，对企业而言，在线的互联网展示已经比打印的广告资料更为重要；[10] 基于国际互联网的通信以及电话服务正以比陆地线路通信速度更快的速度在增长。[11]

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

诸如电子政务[12]、电子商务[13]、电子教育[14]、电子卫生[15]和电子环境等信息通信技术应用，已被人们视为发展的助推器，原因是它们为向偏远和农村地区提供各种各样的基础服务提供了一条有效的渠道。信息通信技术的应用有助于推动《千年发展目标》的实现、减少发展中国家的贫困、改善卫生和环境条件。运用正确的方法、背景和执行过程，在信息通信技术应用与工具中的投资可以带来生产力和质量的提升。反过来，信息通信技术的应用可以释放技术与人类的能力，使基本服务更

具可达性。在这方面，出于犯罪目的、抱着诈骗的意图，借助国际互联网来实施在线的身份盗用和获取他人证书和/或个人信息的行为，现已成为电子政务和电子商务服务进一步发展的主要威胁之一。[16]

国际互联网服务的成本通常也大大低于网络之外可比服务的成本。[17] 与传统的邮政服务相比，电子邮件服务通常是免费的，或者只收取非常少的一点费用。[18] 在线的维基百科服务[19] 也可以免费使用，还包括数百种的在线托管服务。[20] 低成本相当重要，原因是这使得更多的用户可以使用这些服务，包括那些只有有限收入的人们。鉴于发展中国家许多人的财力有限，因此国际互联网使得他们能够使用一些在网络之外无法以如此低廉价格得到的服务。

1.2 优势与风险

在日常生活的诸多方面中引入信息通信技术已经带来信息社会这一现代概念的提出。[21] 信息社会的发展提供了巨大机遇。[22] 无障碍地访问信息有助于民主，原因是信息的流动不受国家政权的控制（如在东欧和北非国家发生过的情况）。[23] 技术发展改善了日常生活 — 例如网上银行和网上购物、移动数据业务和网络协议语音服务（VoIP）的使用，就是信息通信技术如何融入我们日常生活的一些最新发展例子。[24]

不过，信息社会的发展也伴随着新的和严重的威胁。[25] 如今，人类生活中一些必不可少的服务，如供水和供电等，都依赖于信息通信技术。[26] 汽车、交通管制、电梯、空调和电话等，也都依赖于信息通信技术顺畅地发挥其功能。[27] 对信息基础设施和国际互联网服务的攻击现已具有以新的和危险的方式危害社会的可能性。[28]

对信息基础设施和国际互联网服务的攻击已有发生。[29] 网络诈骗和黑客攻击等，只是与计算机有关的犯罪的一些例子，如今，这类犯罪每天都会大量发生。[30] 网络犯罪导致巨额的经济损失。[31] 仅 2003 年一年，恶意软件就造成了高达 170 亿美元的损失。[32] 据估计，2007 年，网络犯罪带来的收入超过了 1 000 亿美元，第一次超过了毒品非法贸易的收入。[33] 2014 年公布的研究结果显示，网络犯罪每年在全球造成的损失可能高达 4 000 亿美元。[34]接近 60%的美国企业认为，网络犯罪比其他物理犯罪对其造成的危害更大。[35] 这些预计清楚地表明了保护好信息基础设施的重要性。[36]

多数上述针对计算机基础设施的攻击不一定专门针对关键基础设施，然而 2010 年发现的“Stuxnet”恶意软件昭显了重点对关键基础设施进行攻击所带来的威胁。[37] 上述具有 4 000 多种功能[38] 的恶意软件重点攻击运行通常用于关键基础设施监控软件的计算机系统。[39]

1.3 网络安全与网络犯罪

在互连环境中，网络犯罪与网络安全问题几乎相生相伴。2010 年联合国大会通过的网络安全决议[40] 将网络犯罪确定为一项主要挑战，这是对这两个问题的极好诠释。

网络安全[41] 在当前的信息技术以及国际互联网服务[42] 的发展中发挥着重要作用。增强网络安全和保护关键的信息基础设施，对各国安全和经济福祉至关重要。使国际互联网更加安全（并且保护国际互联网用户），已经成为新业务发展和各国政策的有机组成部分。[43] 阻止网络犯罪是国家网络安全和关键信息基础设施保护战略的有机组成部分。特别地，这包括采取适当的立法措施，阻止出于犯罪或其他目的滥用信息通信技术，以及防止那些旨在影响国家关键基础设施完整性的行为。在国家层面上，这是一种共同的责任，要求政府主管部门、私营部门和公民各方在防止、预备、响应和恢复网络犯罪方面采取协同行动。在区域和国际层面上，这需要各相关方的合作与协调。因此，在网络安全的国家框架与战略的形成和实施上，需要采取一种综合的方法。[44] 网络安全战略 — 例

如，技术保护系统的研发，或者教育用户如何预防成为网络犯罪的受害者 — 将有助于降低网络犯罪的风险。[45] 制定和支持网络安全战略是在与网络犯罪作斗争的过程中一个至关重要的因素。[46]

由网络安全问题引发的法律上、技术上和制度上的挑战，是全球性的和深远的，并且只有在国际合作的框架内，考虑到不同利益攸关方和现有举措的作用，通过一种一致的战略才能加以解决。[47] 在这方面，信息社会世界峰会（WSIS）[48] 已认识到因网络安全的缺陷和网络犯罪的泛滥而导致的真实而巨大的风险。《信息社会世界峰会信息社会突尼斯议程》[49] 第 108～110 段的规定（包括附录），为利益攸关各方在国际层面上执行《信息社会世界峰会日内瓦行动计划》[50] 制定了一项计划，说明按照十一个行动方面利益攸关各方应采取的实施程序，以及为便于落实各不同行动方面而进行的责任分配。在信息社会世界峰会上，世界各国领导人和政府指定国际电信联盟负责推动信息社会世界峰会 C5 行动方面，即，树立使用信息通信技术的信心和提高安全性的执行工作。[51]

在这方面，国际电信联盟秘书长与来自政府、业界、区域性和国际组织、学术与研究机构的合作伙伴一道，于 2007 年 5 月 17 日发出了《全球网络安全议程》（GCA）。[52] 《全球网络安全议程》是一个有关对话与国际合作的全球框架，旨在协调国际社会对日益严峻的网络安全挑战做出响应，以及增强信息社会的信心和安全。它基于现有的工作、举措和合作关系，目标是提出全球战略，以应对当前与树立使用信息通信技术的信心和提高安全性有关的挑战。在国际电联内，通过在国际合作框架内促进国际电联三个部门对网络安全活动的执行，GCA 补充了现有的国际电联工作计划。

《全球网络安全议程》有七大战略目标，建立在五个工作领域之上：1）法律措施；2）技术与程序措施；3）组织结构；4）能力建设；以及 5）国际合作。[53]

与网络犯罪的斗争需要一种综合的方法。鉴于任何一种技术措施都无法单独防止任何犯罪，因此，允许执行机构对网络犯罪进行有效调查和起诉至关重要。[54] 在 GCA 的工作领域中，“法律措施”着眼于如何应对网络犯罪活动带来的挑战，这些犯罪是以国际兼容的方式、在信息通信技术网络上进行的。“技术与程序措施”着眼于关键举措，以便采取更好的方法，增强和改善网络空间的安全与风险管理，包括认证计划、协议和标准。“组织结构”着眼于预防、探测、响应网络攻击并做好危机管理，包括保护关键的信息基础设施系统。“能力建设”着眼于精心制定有关能力建设机制的战略，以便在国家政策议程中提高意识、传播技能、促进网络安全。最后，“国际合作”着眼于在应对网络威胁中的国际合作、对话和协调。

制定适当的法律以及在这种方法内制定与网络犯罪有关的法律框架，是网络安全战略的一个重要组成部分。这首先要求所有必需的实体刑法条款来对一些行为定罪，如计算机诈骗、非法访问、数据干扰、版权侵权和儿童色情。[55] 事实是，适用于类似之非网络犯罪行为的刑法条款，并不意味着也可适用于国际互联网上的犯罪行为。[56] 因此，对当前的国家法律进行全面彻底的分析，对辨别任何可能存在的差别至关重要。[57] 除了实体刑法条款，[58] 执法机构还需要一些必要的工具和设备来调查网络犯罪，[59] 而此类调查本身就带来了一系列的挑战。[60] 罪犯几乎可以从世界任何地方来实施犯罪行为，并采取措施掩盖其身份。[61] 与那些用来调查普通犯罪行为的工具和设备相比，调查网络犯罪行为所需的工具和设备可能大不相同。[62]

1.4 网络犯罪的国际影响

网络犯罪常常波及国际范围。[63] 带有非法内容的电子邮件，在从发送者传送到接收者的过程中，常常历经许多国家，或者非法内容可以保存在别的国家。[64] 在网络犯罪调查过程中，相关国家之间的密切合作极为重要。[65] 各国之间现有的相互法律援助协议基于正式的复杂的且常常是耗时的程序，且往往并不包含具体针对计算机的调查。[66] 因此，至关重要的是，建立一些有助于对网络犯罪案件迅速做出响应且请求国际合作的程序。[67]

许多国家将其相互法律援助体系建立在“双重犯罪”的原则上。[68] 全球层面上对网络犯罪的调查通常局限于在所有参与国家中已定罪的那些犯罪。尽管许多犯罪行为（如传播儿童色情）可在多数辖区遭到起诉，但区域之间的差别扮演着重要的角色。[69] 诸如仇视演讲等其它类型非法内容即是一个例子。不同国家对非法内容的定罪是有差别的。[70] 在某个国家中可以合法传播的内容，在另一个国家很可能就是非法的。[71]

当前正在使用的计算机技术基本上是世界通用的。[72] 除了语言问题和电源适配器的不同，亚洲和欧洲销售的计算机系统和手机几乎没有什么差别。国际互联网世界也是类似的情形。由于标准化的实施，非洲各国使用的网络协议与美国使用的协议是相同的。[73] 标准化使世界各地的用户能够通过国际互联网接入相同的服务。[74]

问题是全球技术标准的统一对国家刑法的发展将产生怎样的影响。就非法内容而言，国际互联网用户可以从世界各地访问信息，这样，他们能够访问在国外属于合法而在本国属于非法的信息。

理论上，来自技术标准化的发展远超过了技术与服务的全球化，并且可能导致各国法律的调和。不过，正如在欧洲理事会《网络犯罪公约》第一议定书（《网络犯罪公约》）的谈判过程中所显示的那样，[75] 国家法律原则的变化远比技术发展的步伐慢得多。[76]

尽管国际互联网并不认可国界控制，但的确存在一些手段可限制对特定信息的访问。[77] 接入提供商通常可以阻止某些网站，而保存了某一网站的服务提供商，可以根据与某一特定国家相关联的 IP 地址，阻止那些用户访问其信息（“IP 筛选”）。[78] 两种措施都可以被绕开，但是不管怎样，它们是可以用来在全球网络中保持地区差别的手段。[79] 开放网络倡议[80] 报告说，全世界约有二十四个国家实施这种审查制度。[81]

1.5 对发展中国家的影响

寻求应对网络犯罪威胁的战略与解决方案是一个重大挑战，对于发展中国家尤其如此。综合的反网络犯罪战略通常包括技术保护措施以及法律手段。[82] 这些手段的制定与实施需要时间。技术保护措施尤其需要高额的成本。[83] 发展中国家需要从一开始就将保护措施溶入到国际互联网的普及中，原因是，尽管这可能在最初提高国际互联网服务的成本，但从长期看，由于避免了因网络犯罪而造成的巨大费用和破坏，其收益将大大超过任何技术保护措施和网络安全防卫措施的初始成本。[84]

事实上，由于发展中国家不太严格的安全和防护措施，因此与脆弱的保护措施有关的风险可能更严重地影响到它们。[85] 有能力保护客户和公司，不仅仅是一项针对日常业务的基本要求，也是针对在线或基于国际互联网业务的基本要求。如果缺乏国际互联网安全性，发展中国家可能在推动电子商务和进军在线服务行业等方面遭遇巨大困难。

发展有助于网络安全的技术措施以及制定适当的有关网络犯罪的法律，对发达国家和发展中国家都至关重要。相比之后才在计算机网络中采取安全和保护措施所耗费的成本，一开始就采取网络安全防护措施其成本将低廉得多。发展中国家需要将其反网络犯罪战略在一开始就与国际标准统一起来。[86]

1 On the development of the Internet, see: Yang, Miao, ACM International Conference Proceeding Series; Vol. 113;roceedings of the 7th International Conference on Electronic Commerce, page 52 – 56; The World Information Society Report 2007, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/. According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information, see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

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

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

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

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

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

[7] Current reports highlight that around 11 per cent of the African population has access to the Internet. See www.internetworldstats.com/stats1.htm.

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

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

[10] Regarding the ability to block Internet-based information services by denial-of-service attacks, see below: § 2.5.5.

[11] Regarding the related difficulties of lawful interception of Voice over IP communication, see: *Bellovin and others*, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP", available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, "Voice over IP: Forensic Computing Implications", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[12] Related to risks and challenges see for example: *Choudhari/Banwet/Gupta*, Identifying Risk Factors in for E-governance Projects, published in Wgarwal/Ramana, Foundations of E-government, 2007, page 270 et. seq; *Ndou*, E-Government for Developing Countries, Opportunities and Challenges, DJISDC 2004, 18, page 1 et seq.

[13] See for example: *Ekundayo/Ekundayo*, Capacity constraints in developing countries: a need for more e-learning space? The case of Nigeria, Proceedings ascilite Auckland, 2009, page 243 et seq.

[14] See for example: *Ekundayo/Ekundayo*, Capacity constraints in developing countries: a need for more e-learning space? The case of Nigeria, Proceedings ascilite Auckland, 2009, page 243 et seq.

[15] See for example: *Aggarwal,* Role of e-Learning in A Developing Country Like India, Proceedings of the 3rd National Conference, INDIA, Com 2009.

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

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

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

[19] www.wikipedia.org

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

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

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

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

[24] Regarding the extent of integration of ICTs into the daily lives and the related threats, see: § 3.2.1 below, as well as *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

[25] See UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211, page 1; *Sieber*, The Threat of Cybercrime, Organised crime in Europe: the threat of Cybercrime, page 212; ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

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

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

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

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

[30] The Online-Community HackerWatch publishes reports on hacking attacks. Based on their sources, more than 219 million incidents were reported in one month (November 2010). Source: www.hackerwatch.org. Regarding the necessary differentiation between port scans and possible attempts to break into a computer system, see:

Panjwani/Tan/Jarrin/Cukier, An Experimental Evaluation to Determine if Port Scans are Precursors to an Attacks, available at: www.enre.umd.edu/faculty/cukier/81_cukier_m.pdf.

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

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

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

34 Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014.

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

36 *Wilshuse*n, Internet Infrastructure, Challenges in Developing a Public/Private Recovery Plan, Testimony before the Subcommittee on Information Policy, 2007, GAO Document GAO-08-212T, available at: www.gao.gov/new.items/d08212t.pdf. For more information on the economic impact of cybercrime, see below: § 2.4.

37 Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

38 Cyber Security Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

39 *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Under the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

40 UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

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

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

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

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

45 For more information, see: *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1.

46 See: *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, available at: www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Harmonizing_National_and_Legal_Approaches_on_Cybe

rcrime.pdf; see also: Pillar One of the ITU Global Cybersecurity Agenda, available at: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html. With regard to the elements of an anti-cybercrime strategy, see below: §4.

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

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

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

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

51 For more information on WSIS Action Line C5: Building confidence and security in the use of ICTs, see: www.itu.int/wsis/c5/

52 For more information on the Global Cybersecurity Agenda (GCA), see: www.itu.int/cybersecurity/gca/

53 For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

54 For an overview of the most important instruments in the fight against cybercrime, see below: § 6.5.

55 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, 141. For an overview of the most important substantive criminal law provisions, see below: § 6.2..

56 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, 245 *et seq.*

57 For an overview of cybercrime-related legislation and its compliance with the best practices defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No.3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

58 See below: § 6.2.

59 See below: § 6.5.

60 For an overview of the most relevant challenges in the fight against cybercrime, see below: § 3.2.

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

62 Regarding legal responses to the challenges of anonymous communication, see below: § 6.5.12 and § 6.5.13.

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

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

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

66 See below: § 6.5.

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

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

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

[70] The different legal traditions with regard to illegal content was one reason why certain aspects of illegal content are not included in the Council of Europe Convention on Cybercrime, but addressed in an additional protocol. See below: § 5.2.1.

[71] With regard to the different national approaches towards the criminalization of child pornography, see for example: *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, 1999.

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

[73] The most important communication protocols are TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks, 2002; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture, 2006.

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

[75] Additional Protocol to the Convention on cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (CETS No. 189), available at: www.conventions.coe.int.

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

[77] See: *Zittrain*, History of Online Gatekeeping, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf.

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

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

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

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

[82] See below:§ 4.

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

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

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

[86] For more details about the elements of an anti-cybercrime strategy, see below:§ 4.

2. 网络犯罪现象

2.1 定义

参考书目（节选）： *Carter*, Computer Crime Categories: How Techno-Criminals Operate, FBI Law Enforcement Bulletin, 1995, page 21, available at: www.fiu.edu/~cohne/Theory%20F08/Ch%2014%20-%20Types%20of%20computer%20crime.pdf; *Charney*, Computer Crime: Law Enforcement's Shift from a Corporeal Environment to the Intangible, Electronic World of Cyberspace, Federal Bar News, 1994, Vol. 41, Issue 7, page 489 et seq., *Chawki*, Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview/; *Forst*, Cybercrime: Appellate Court Interpretations, 1999, page 1; *Goodman*, Why the Policy don't care about Computer Crime, Harvard Journal of Law & Technology, Vol. 10, No. 3; page 469; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No.2, page 144; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Hale*, Cybercrime: Facts & Figures Concerning this Global Dilemma, CJI 2002, Vol. 18, available at:

www.cjcenter.org/cjcenter/publications/cji/archives/cji.php?id=37; *Hayden*, Cybercrime's impact on Information security, Cybercrime and Security, IA-3, page 3; *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004; *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf.

关于网络犯罪的大多数报告、指南或出版物都以定义“计算机犯罪”和“网络犯罪”[87]这两个术语[88]开始。

近几十年来，已采用了多种不同方式制定这两个术语的确切定义。[89]明确“网络犯罪”与“计算机相关犯罪”之间的关系十分有益。[90]在不探究细节的前提下，“网络犯罪”比“计算机相关犯罪的含意更窄，因为它涉及计算机网络。计算机相关犯罪甚至包含与网络无关、仅影响独立计算机系统的犯罪。在联合国第 10 届预防犯罪和罪犯待遇大会期间，在相关讲习班范围内确定了两个定义：[91]狭义的网络犯罪（计算机犯罪）系指以电子操作手段针对计算机系统及其所处理数据安全的任何非法行为。广义的网络犯罪（计算机相关犯罪）系指以计算机系统或网络、或以关系到计算机系统或网络的手段做出的任何非法行为，包括通过计算机系统或网络非法拥有、提供或发布信息。[92]

一种常见的定义是将网络犯罪描述成以计算机或网络为工具、目标或地点的任何犯罪活动。[93]这种广泛定义存在若干困难。例如，如果罪犯间或利用键盘袭击或杀死受害人，则该定义包含传统的谋杀罪。另一个广泛定义是《加强预防网络犯罪和恐怖主义国际公约斯坦福公约》（《斯坦福公约》[94]第 1.1 条中的定义，它将网络犯罪定义为涉及网络系统的犯罪行为。[95]

有些定义试图将网络犯罪的目标或意图考虑进来，对网络犯罪做更准确的定义，[96]例如，“非法的或被某些团体视为不正当的、可以通过全球电子网络实施的、由计算机策划的行为。”[97]这些更加精确的描述没有包括那些利用物理硬件来实施的普通犯罪，而这存在一定风险，因此这些犯罪行为有可能被一些国际协议认定为网络犯罪，如《英联邦计算机和计算机相关犯罪示范法》或[98]《欧洲理事会《网络犯罪公约》》。举例而言，若某人生产包含恶意软件的 USB[99]设备，当该设备被连接时对计算机数据造成破坏，那么认为他的行为即是《网络犯罪公约》第 4 条定义的犯罪行为。[100]不过，根据以上狭义定义，没有通过全球电子网络进行的、使用物理设备来删除数据以复制

恶意代码的行为，将不被定性为网络犯罪。而根据更宽泛的描述和定义，不仅这种行为被定义为网络犯罪，而且包括如非法的数据干扰等行为也被定义为网络犯罪。

多样的方式和与之相伴的各种问题表明，在定义“计算机犯罪”和“网络犯罪”这两个术语上，存在相当大的困难。[101] “网络犯罪”这一术语用于描述一系列的犯罪行为，包括传统的计算机犯罪以及网络犯罪。由于这些犯罪行为在许多方面存在差异，因此没有哪一种单独的准则能够将不同区域和国际法律以方式中提到的所有行为都包括在内，且不包括那些只是使用硬件实施的传统的犯罪行为。事实上，只要这一术语不是用作法律术语，那么没有“网络犯罪”的单一定义并不重要。[102] 下列各章将以与类型相关的方式为基础，而不述及任何定义。

2.2 网络犯罪类型

参考书目： Big Data for Development: Challenges & Opportunities, UN Global Pulse, 2012; *Chawki,* Cybercrime in France: An Overview, 2005, available at: www.crime-research.org/articles/cybercrime-in-france-overview; *Gordon/Ford*, On the Definition and Classification of Cybercrime, Journal in Computer Virology, Vol. 2, No. 1, 2006, page 13-20; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2003, available at: www.ncjrs.gov/pdffiles1/nij/grants/198421.pdf; *Hartmann/Steup,* The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment, published in Podins/Stinissen/Maybaum, 5th International Conference on Cyber Conflicts, 2013; *Kim/Wampler/Goppert/Hwang/Aldridge,* Cyber attack vulnerabilities analysis for unmanned aerial vehicles, American Institute of Aeronautics and Astronautics, 2012; *Sircar*, Big Data: Countering Tomorrow’s Challenges, Infosys Labs Briefings, Vol. 11, No. 1, 2013; *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004.

“网络犯罪”这一术语包括一系列犯罪行为。[103] 公认的犯罪行为涵盖众多的犯罪行为，因此难以为网络犯罪制定一套分类或归类体系。[104] 可以在《网络犯罪公约》中找到一种方式，[105] 该方式对以下四种类型的犯罪行为做了区分[106]:

1. 破坏计算机数据与系统机密性、完整性和可用性的攻击行为；[107]
2. 与计算机有关的攻击行为；[108]
3. 与内容有关的攻击行为；[109] 以及
4. 与版权有关的攻击行为；[110]

这种分类整体上并不一致，原因是它没有基于一个单独的标准来区分各个类别。三个类别着重强调法律保护的目标：“破坏计算机数据与系统机密性、完整性和可用性的攻击行为”；[111] 与内容有关的攻击行为；[112] 以及与版权有关的攻击行为。[113] 第四个类别“与计算机有关的攻击行为”[114] 不是着重于法律保护的目标，而是着眼于犯罪方法。这种不一致性导致各类别之间存在一定的重叠。

此外，用于描述犯罪行为的一些术语（例如“网络恐怖主义”[115] 或者“网络钓鱼”[116]），涵盖了可同时归入几个类别的犯罪行为。尽管如此，上述四种分类仍是讨论网络犯罪现象的有用依据。

2.3 确定计算机犯罪和网络犯罪

自信息技术问世以来，有关以犯罪方式滥用该技术以及做出必要的法律对策问题一直得到讨论。近 50 年来，在国家和区域层面已实施了繁覆多样的解决方案。该议题依然充满挑战的原因之一是因为技术不断发展变化，同时犯罪方式方法也在持续演变。

2.3.1 二十世纪 60 年代

二十世纪 60 年代，继真空管技术之后的规模更小和更加廉价的晶体管计算机系统的引入大大增加了计算机技术的使用。[117]在该初期阶段，犯罪行为着眼于对计算机系统和存储数据造成实际破坏。[118]其中得到报告的事件包括 1969 年在加拿大出现的学生暴动导致火灾的发生，毁坏了在大学托管的计算机数据。[119]二十世纪 60 年代中期，美国开始进行有关建立服务于各个部委的中央数据存储管理部门的讨论，[120]在此方面，还讨论了以犯罪方式滥用数据库[121]和对隐私产生的相关风险[122]的问题。[123]

2.3.2 二十世纪 70 年代

二十世纪 70 年代，计算机系统和计算机数据的使用进一步加大。[124]据估计，截至 70 年代末，美国约有 100 000 台大型计算机在运行。[125]随着价格的下降，计算机技术由政府部门、企业和普通公众广为使用。在针对计算机系统的犯罪方面，二十世纪 70 年代的特点是由二十世纪 60 年代的主要针对计算机财产的传统犯罪[126]转向新形式的犯罪。[127]尽管此时以犯罪方式滥用计算机系统并对其造成实际损害依然猖獗，[128]但也出现了新形式的计算机犯罪，其中包括非法使用计算机系统[129]和操纵[130]电子数据。[131]从手工操作交易向计算机操作交易的过渡带来了另一种新的犯罪形式 – 计算机相关欺诈。[132]此时，计算机相关欺诈造成的损失已达到数百万美元。[133]计算机相关欺诈带来了实实在在的特殊挑战，因此执法机构调查的案件日益增多。[134]由于将现有立法用于计算机犯罪案件存在困难，[135]因此人们在世界不同地方开始了有关法律解决方案的讨论。[136]美国讨论了一项专门针对网络犯罪的议案草案。[137]国际刑警组织（Interpol）讨论了相关现象以及做出法律对策的可能性。[138]

2.3.3 二十世纪 80 年代

在二十世纪 80 年代，个人计算机不断普及。随着这一发展，罪犯瞄准的计算机系统数量和潜在的目标数量进一步增加。在该阶段，一系列广泛的关键基础设施首次成为了罪犯攻击的目标。[139]计算机系统普及的一个副作用是人们对软件的兴趣不断加大，从而导致首次出现软件盗版和与专利相关的犯罪行为。[140]计算机系统的互连也带来了新型犯罪。[141]由于网络的存在，因此犯罪分子无需出现在犯罪现场即可进入计算机系统。[142]此外，通过网络分发软件也为犯罪分子传播恶意软件带来了便利，由此发现的计算机病毒日益增多。[143]针对这些情况，各国开始更新其立法，以满足不断变化的犯罪环境提出的要求，[144]相关国际组织也参与了这一进程。经合发组织[145]和欧洲理事会[146]都成立了旨在分析相关现象并对可行的法律对策做出评估的研究组。

2.3.4 二十世纪 90 年代

二十世纪 90 年代出现的图形界面（“WWW”）以及随后的互联网用户数量的急剧增长都带来了新的挑战。在一个国家合法提供的信息可在全球获得 – 甚至包括此类信息的发布被定为犯罪的国家。[147]在调查传统犯罪过程中特别具有挑战性的、与在线服务有关的另一个问题是信息交流的速度问题。[148]最后，儿童色情内容的传播由书籍和磁带的实际交换变为通过网站和互联网服务在线发布。[149]尽管总体而言，计算机犯罪局限于本地，但互联网将电子犯罪变为了跨国界犯罪。有鉴于

此，国际社会开始更加专注地处理这一问题，联合国大会于 1990 年通过的第 45/121 号决议[150]和于 1994 年发布的计算机相关犯罪的预防与监控手册即是其中的两个示例。[151]

2.3.5 二十一世纪

如同此前每个十年一样，二十世纪也目睹了在计算机犯罪和网络犯罪方面出现的新趋势。新千年的头一个十年中，犯罪手段花样繁新、技术精尖，其中包括“网络钓鱼”[152]和“僵尸攻击”[153]，并开始使用执法机构更加难以处理和调查的技术，如“IP 语音（VoIP）通信”[154]和“云计算”[155]。不仅犯罪手法发生变化，其影响也与此前大不相同。由于罪犯能够实现攻击的自动化，因此犯罪数量不断增加。各国以及区域性和国际组织均对日益严峻的挑战做出了响应，并对网络犯罪响应予以高度优先。诸如“大数据[156]”、“无人机[157]”和“可穿戴设备”等新发展则是罪犯在未来最有可能以身试法的重点领域。

2.4 网络犯罪行为的程度和影响

参考书目（节选）： Alvazzi del Frate, Crime and criminal justice statistics challenges in Harrendorf/ Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/ International_Statistics_on_Crime_and_Justice.pdf; Collier/Spaul, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; Hyde-Bales/Morris/Charlton, The police recording of computer crime, UK Home Office Development and Practice Report, 2004; Maguire in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 et seq., available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf; Mitchison/Urry, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; Osborne/Wernicke, Introduction to Crime Analysis, 2003, page 1 et seq. available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

犯罪统计数据可成为学术界和政策制定机构进行讨论并着手开始决策程序的基础。[158]此外，获得有关网络犯罪真实程度的确切信息有助于执法机构完善打击网络犯罪战略、阻止潜在的攻击，并制定更加适当和有效的法律。然而，仅根据特定时间范围内的犯罪数量难以量化网络犯罪对社会产生的影响。[159]此类数据通常源自犯罪统计数据和调查，[160]但将源自这两个渠道的数据用于制定政策建议时往往会带来挑战。

2.4.1 犯罪统计数据

以下数字节选自国家犯罪统计数据。正如以下进一步讨论的那样，这些数字一不代表全球网络犯罪的发展情况，二不代表国家层面网络犯罪的真实程度，在此提出这些数字仅在于使读者了解相关国家的信息。

- 2013 年美国互联网投诉中心所报告的损失与 2012 年相比，增加了 48.8%。[161]
- 德国犯罪统计数据表明，与 2012 年相比，2013 年互联网相关犯罪总数量增加了 12.2%。[162]

目前尚不清楚这些统计数据的代表性如何，也不清楚这些数据是否提供了有关犯罪程度的可靠信息。[163]以犯罪统计数据为基础确定全球网络犯罪威胁存在若干困难。[164]

首先，犯罪统计数据通常在国家层面产生，因此不能从国际层面反映问题的范围。虽然理论上可以将现有数据加以合并，但这一方式仍然不能产生可靠信息，因为各国的立法和记录惯例不尽相同。[165]将不同国家的犯罪统计数据予以合并和比较需要有某种程度的相互兼容性，[166]而在网络犯罪方面恰恰缺乏这种兼容性。即使网络犯罪数据得到记录，但不一定作为单独数字列出。[167]此外，统计数据仅涵盖得到发现和报告的犯罪行为。[168]在网络犯罪方面，人们特别的担心是未得到报告的案件数量极大，[169]其中一个原因可能是企业担心对此做出报告会对企业产生负面宣传作用，从而损害其声誉。[170]如果一家公司对外宣布说黑客访问了该公司的服务器，则客户可能对其失去信心，由此产生的全部代价和后果可能超过黑客攻击造成的损失。另一方面而言，如果罪犯得不到报告和惩处，则他们可能再次犯罪。受害方可能不相信执法部门能够找到罪犯。[171]网络犯罪数量巨大，而得到成功查处的案件却凤毛麟角，通过这一比较，受害方认为对犯罪行为做出报告几乎没有意义。[172]由于自动化攻击便于网络罪犯采用“通过大量的、针对小数额攻击（如预付费欺诈[173]）获得巨大利益的战略，因此未得到报告的犯罪产生的影响可能十分巨大。对于仅仅是小数额的攻击，受害方可能不希望进入耗时的报告程序，得到报告的案件往往是涉及巨大数额的案件。[174]

总而言之，统计信息对于引起人们对该问题不断加剧的影响的注意十分有益，但必须指出，网络犯罪方面的一个主要挑战是缺乏有关该问题的程度以及罪犯被捕、被起诉和被判决方面的可靠信息。如上所述，犯罪统计数据往往不将犯罪行为单独列出，因此现有的有关网络犯罪影响的统计数据总体无法提供政策制定机构所需的有关犯罪行为范围和程度的可靠数据。[175]没有此类数据，很难量化网络犯罪对社会的影响，并相应制定解决该问题的战略。[176]尽管如此，统计数据可成为确定趋势的基础（通过比较若干年的结果即可找出趋势），并成为有关报告网络犯罪程序的指南。[177]

2.4.2 调查

以下数字节选自不同调查。正如以下进一步讨论的那样，这些数字不一定具有代表性，在此提出这些数字仅在于使读者了解此类调查的结果。

- 地下经济服务提供商通告的、最爱人欢迎的信息是信用卡和银行账户信息，其价格在 0.85-30 美元（一份信用卡信息）至 15-850 美元（一份银行账户信息）之间。[178]
- 2007 年，美国第一大互联网诡计为拍卖欺诈，平均每案件造成的损失超过 1 000 美元。[179]
- 2005 年，美国与身份相关的犯罪造成的损失达到 566 亿美元。[180]
- 爱尔兰各种不同网络犯罪案件造成的经济和个人损失差异极大，平均损失为 250 000 欧元以上。[181]
- 一家计算机安全公司在一个季度内即创建了 450 000 多个新的恶意代码签名。[182]
- 参加 2010 年发出的一项问卷调查的所有公司中的四分之一报告说遭受过由网络犯罪造成的运营损失。[183]
- 2004-2008 年，由专业人士报告的拒绝服务和计算机病毒攻击数量已有下降。[184]
- 2009 年，美国、中国、巴西、德国和印度是报告恶意活动最多的前几个国家。[185]
- 2014 年，网络犯罪在全球造成的损失估计介于 3750 亿至 5750 亿美元之间。[186]
- 德国是受网络犯罪影响最严重的的国家，相关损失估计相当于整个国内生产总值（GDP）的 1.6%。[187]美国因此遭受的损失估计为 GDP 的 0.64%，巴西为 0.32%，肯尼亚为 0.01%。[188]

- 数据泄漏的平均成本为人均 136 美元。[189]一次与客户数据库相关的黑客攻击为索尼公司带来了约 1.7 亿 美元的直接成本。[190]

利用此类调查确定网络犯罪的程度和影响存在若干令人担心的问题。

提供可靠的经济损失估算极为困难。某些渠道估计，美国的企业和机构[191] 一年中因网络犯罪而造成的损失高达 670 亿美元之多；不过，难以肯定对抽样调查结果所做的推断是否合理。[192] 对这种方法论的批判不仅适用于损失，而且适用于公认的攻击数量。

与统计信息有关的另一个困难是，不可靠或未得到核实的信息被反复引用，其中一个示例涉及互联网儿童色情商业方面的统计信息。例如，若干分析人士引用说，据 TopTenReviews 估计，互联网儿童色情每年在全世界产生 25 亿美元的收入。[193]然而 TopTenReviews 不提供有关如何进行调查的背景信息。TopTenReviews 在其网站上声称“该公司为您提供做出明智购买所需的信息。我们对每一类别的最佳产品均提出建议。通过展品对比图、新闻、文章和视频，我们简化消费者的程序”，人们对使用此类数据可能十分担忧。另一个引用未对参考资料中的数字进行核实的示例是华尔街日报 2006 年发现的示例。[194]该报的一名记者在调查一项有关儿童色情数百亿美元业务（一年 200 亿美元）的引用时报告说，有两份主要文件包含有关收入为 30 亿至 200 亿美元的信息 – 一份为 NCMEC 的出版物，另一份为欧洲理事会的出版物，该记者谈到，上述两个机构未对这些数字予以确认。

由于调查往往仅包含事件而不提供进一步的信息或细节，因此难以据此得到有关趋势方面的结论。一个例子是美国计算机安全协会（CSI）[195] 于 2007 年进行的计算机犯罪与安全调查，该调查分析的趋势包括与计算机有关的攻击行为的数量。[196] 调查基于来自美国公司、政府机构和金融机构 494 个计算机安全从业者的回复。[197] 调查文件记录了答复者报告的、在 2000 年至 2007 年之间发生的攻击行为数量。调查结果显示，自 2001 年以来，经历并承认受到过病毒攻击或非授权信息访问（或系统渗透）的答复者的比例下降了。调查结果没有解释为什么出现了这种下降趋势。

关于网络犯罪的调查无法提供有关攻击行为程度或范围的可靠信息。[198] 由于无法确定攻击对象报告的攻击程度，[199] 以及由于以下事实，即无法找到关于网络犯罪数量减少的合理解释，因此，这些统计数据可任由人们解读。目前，没有足够的证据来预测未来的趋势和发展。

2.5 破坏计算机数据与系统机密性、完整性和可用性的犯罪行为

参考书目（节选）： Chawki/Abdel Wahab, Identity Theft in Cyberspace: Issues and Solutions, page 17, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; Ealy, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf; Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; Goodman/Brenner, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; Hackworth, Spyware, Cybercrime & Security, IIA-4; Kabay, A Brief History of Computer Crime: An Introduction for Students, 2008; Ollmann, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; Paxson, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; Sieber, Council of Europe Organised Crime Report 2004; Szor, The Art of Computer Virus Research and Defence, 2005; Urbas/Krone, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html; Walden, Computer Crimes and Digital Investigations, 2006, Chapter 3.250; Yee, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 et seq.

归入这一类别的所有攻击行为，都是针对机密性、完整性和可用性这三条法律原则中的（至少）一条。与数个世纪以来刑法中所涵盖的犯罪（如盗窃和谋杀）不同，犯罪行为的计算机化出现的时间相对较晚，原因是计算机系统和计算机数据的发展只是大约 60 年前的事情。[200] 对这些犯罪行为进行有效的起诉要求现有的刑法条款不仅保护有形的实体和物理文件不被操纵，而且还要延伸至纳入这些新的法律原则。[201] 本小节对这一类别中包含的、最常见的攻击行为做一概述。

2.5.1 非法访问（黑客行为、骇客行为）[202]

描述为“黑客行为”的攻击行为指的是非法访问计算机系统，[203] 这是一种最早出现的、与计算机有关的犯罪行为。[204] 随着计算机网络的发展（特别是国际互联网），这种犯罪行为已经变得日益普遍。[205] 黑客攻击的一些著名对象包括美国国家航空航天局（NASA）、美国空军、五角大楼、雅虎、谷歌、易趣（eBay）以及德国政府等。[206]

黑客攻击的例子包括破解受到密码保护的网站的密码[207]；以及绕过计算机系统的密码保护。但“黑客”行为也包括准备行为，如，使用有缺陷的硬件或执行有缺陷的软件来非法获取密码以进入计算机系统；[208] 创建“诱骗”网站以使用户泄露其密码，[209] 以及安装基于键盘记录方法的硬件和软件（如“键盘记录器”）、以记录每一次键盘敲击 — 并因此盗取在计算机和/或设备上使用的任何密码。[210]

攻击者的动机各不相同。一些攻击者将其行为局限于绕过安全措施的活动，只是为了证明自己的能力。[211] 其他攻击者的行为带有政治意图（称为“黑客行动主义”[212]） — 一个例子是最近攻击联合国主要网站的事件。[213] 在大多数情况下，攻击者的动机不会仅限于不正当地访问计算机系统。攻击者利用这种访问来实施进一步的犯罪，如数据刺探、数据操纵或拒绝服务（DoS）攻击。[214] 在许多情况下，对计算机系统的非法访问只是网络犯罪至关重要的第一步。[215]

许多分析人士认识到，试图非法访问计算机系统事件的数量正在增加，仅 2007 年 8 月一个月，全世界就报告了超过 2500 万件此类案件。[216] 导致黑客攻击案件数量增加的主要因素有三个：计算机系统的保护措施不力和不完备、可自动发起攻击的软件工具的开发、作为黑客攻击目标的私人计算机所发挥的日益大的作用。

计算机系统的保护措施不力和不完备

全世界有数亿台计算机与国际互联网连接，许多计算机系统不具备适当的保护措施以防止非法访问。[217] 美国马里兰大学进行的一项分析表明，连接到国际互联网的、未采取保护措施的计算机系统，有可能在不到一分钟的时间内就遭到攻击。[218] 安装保护措施可以降低被攻击的风险，但对那些具有良好保护措施的计算机系统进行的成功攻击证明，技术保护措施绝不能彻底阻止攻击。[219]

自动攻击软件工具的发展

最近，正用软件工具来自动发起攻击。[220] 在软件和预先设定的攻击的帮助下，单独一个攻击者可以使用一台计算机、在一天内向数千台计算机系统发动攻击。[221] 如果攻击者访问更多的计算机 — 例如通过僵尸网络 [222] — 则他/她可以进一步扩大攻击范围。由于这些软件工具中的大多数使用预先设定的攻击方法，因此并非所有的攻击都证明是成功的。定期更新操作系统和软件应用程序的用户，可以降低其成为这些大规模攻击的受害者的风险，原因是开发保护软件的公司对攻击工具进行了分析，并对标准化的黑客攻击行为有所防范。

高调攻击常常基于个别设计的攻击。这些攻击之所以成功，并不是采用了什么高精尖方法的结果，而在于被攻击计算机系统的数量。能够实现这些标准化攻击的工具在国际互联网上随处可见，[223] 有些是免费的，但有效的工具往往要花费几千美元。[224] 一个例子是一种可以使攻击者定义一个 IP 地址范围（例如从 111.2.0.0 到 111.9.253.253）的黑客攻击工具。这些软件能够对使用其中一个定义之 IP 地址的所有计算机的未保护端口进行扫描。[225]

在黑客战略中私人计算机日益成为攻击目标

访问一个计算机系统通常并不是攻击的主要动机。[226] 由于企业计算机通常比私人计算机保护得更好，因此，更难使用预先配置的软件工具对企业计算机实施攻击。[227] 过去几年间，攻击者逐渐将其攻击对象指向私人计算机，原因是许多私人计算机都没有采取足够的保护措施。此外，私人计算机通常包含敏感信息（例如信用卡和银行账户细节）。攻击者也以私人计算机为目标，是因为在一次成功的攻击之后，攻击者可以将这台计算机纳入其僵尸网络中，并将其用于实施进一步的犯罪活动。[228]

非法访问计算机系统可被视为与非法闯入某一建筑物相类似，在许多国家，这被认为是刑事犯罪行为。[229] 对非法访问计算机行为的定罪有许多不同方法，对这些方法的分析表明，在某些情况下制定的法律条款将非法访问与随后的攻击行为混为一谈，或者试图将非法访问的定罪仅仅限制为严重违法而已。有些规定只对最初的访问定罪，而其他方法仅将刑事犯罪限于被访问的系统受到安全措施的保护，[230] 或攻击者具有恶意，[231] 或获取、修改或破坏了数据。其他的法律体系不对单纯的访问予以定罪，而着重于随后的攻击行为。[232]

在黑客战略中私人计算机日益成为攻击目标：

近期的分析结果表明，除前几十年肆虐一时的广泛和大规模攻击外，网络攻击目前呈现出更加精密和更有针对性之势。[233]大规模攻击采取的是投机取巧的方法，执行起来相对容易，但有针对性的攻击将需要罪犯投入更多精力，其效果更显著，给受害者[234]造成的损失[235]也更大。

2.5.2 非法数据获取（数据刺探）

计算机系统中常常保存有敏感信息。如果计算机系统与国际互联网相连，那么攻击者可以借助国际互联网，从世界几乎任何地方试图访问到这些信息。[236] 国际互联网越来越多地用于获取贸易秘密。[237] 敏感信息的价值以及远程访问之的能力使得数据刺探变得令人兴趣十足。二十世纪 80 年代，一些德国的黑客成功地进入到了美国的政府和军事计算机系统，获取了秘密情报并将它们卖给了不同国家的情报机构。[238]

攻击者使用各种各样的技术来访问受害者的计算机，[239] 包括：利用软件来扫描未保护的端口，[240] 利用软件来绕过保护措施，[241] 以及运用“社会工程”。[242] 尤其是最后一种方法“社交工程”，指的是一种非技术型的入侵方法，它在很大程度上依赖于人的互动，通常引诱人们违反正常的安全程序，因此格外有趣，原因是它不基于技术性手段。[243] 在非法访问方面，它描述了对人的操纵，意图是获得对计算机系统的访问。[244] 社会工程通常极为成功，原因是计算机安全中最薄弱的环节常常就是操作计算机系统的用户。例如，“网络钓鱼”最近成为网络空间中一种重要的犯罪行为，[245] 它指的是试图以欺诈手段获取敏感的信息（如密码），方法是在看似正式的电子通信中，伪装成一个可信任的人或者一家可信任的企业（如金融机构）来实施欺诈。

尽管用户在人性方面的弱点为网上实施欺骗打开了方便之门，但它也提供了解决方案。经过良好教育的计算机用户不会轻易成为采用社交工程攻击者的受害对象。因此，用户教育是任何一种反网络犯罪战略的重要组成部分。[246] 此外，可采用技术措施预防非法访问。经济合作与发展组织

（OECD）强调用户使用加密技术的重要性，原因是加密技术有助于加强数据保护。[247] 如果存储信息的个人或组织使用适当的保护措施，那么密码保护措施将比任何物理的保护措施都更为有效。[248] 攻击者成功获取敏感信息常常是由于被攻击对象缺少保护措施。由于越来越多的重要信息存储于计算机系统，因此评估用户的技术保护措施是否充分，或法律制定者是否需要对数据刺探予以定罪、以增加保护即变得必不可少。[249]

尽管攻击者通常以商业秘密为目标，但保存在私人计算机上的数据也正日益成为攻击对象。[250] 个人用户通常会在其计算机上保存银行账户和信用卡信息。[251] 攻击者可以将这些信息用于其自身目的（例如，获取银行账户详细信息以转移资金）或者将其卖给第三方。[252] 例如，信用卡记录的出售价格可高达 60 美元。[253] 黑客对私人计算机的关注非常有趣，原因是来自商业秘密的利润通常高于靠获取或出卖私人信用卡信息而获得的利润。不过，由于私人计算机通常缺乏严密的保护，因此对私人计算机进行数据刺探可能变得更加有利可图。

获取信息的手段有两种：罪犯访问计算机系统或数据存储设备并获取信息；或者运用操纵方法来使用户泄露信息或访问代码，使攻击者能够访问信息（“网络钓鱼”）。

攻击者常常使用安装在受害者计算机上的计算机工具或者一种称为“刺探程序”的恶意软件来向自己传输数据。[254] 最近几年，出现了各种类型的刺探程序，如键盘记录器。[255] 键盘记录器是一种记录受感染计算机的键盘上每一次键盘敲击的软件工具。[256] 有些键盘记录器只要受害者的计算机连接到国际互联网，便可向攻击者发送所有记录的信息。另一些键盘记录器对记录的数据进行初步整理和分析（例如，只选取可能是信用卡信息的数据 [257]），并只传输发现的重要数据。类似的设备也可以像硬件设备一样插入键盘与计算机系统之间，以记录键盘上的敲击。基于硬件的键盘记录器更难安装和检测，原因是它们需要以物理方式接入计算机系统。[258] 不过，传统的反刺探程序和反病毒软件基本上无法识别它们。[259]

除了访问计算机系统，攻击者还可以通过操纵用户来获取数据。最近，攻击者研发了一些有效的欺骗诡计来获取秘密信息（如银行账户信息和信用卡数据），方法是利用社交工程技术来操纵用户。[260] 最近，“网络钓鱼”已成为与网络空间有关的一种最重要的犯罪行为。[261] “网络钓鱼”这一术语用于描述这样一种犯罪类型，即它试图通过欺诈手段来获取敏感信息，例如，在看似正式的电子通信中通过伪装成一个可信任的人或一家可信任的企业（如金融机构）来获取密码等。[262]

在“大数据”等环境中，公司为进行复杂分析往往收集大量数据，在网络威胁环境中，此类发展改变了数据泄露的现实后果。若罪犯可访问存储了客户个人数据的大型数据库，则仅仅数据泄露本身便可能致使相关公司蒙受巨额损失—即使在罪犯并未使用数据为非作歹的情况下亦是如此。[263] 数据泄漏的平均成本为人均 136 美元。[264]一次与客户数据库相关的黑客攻击为索尼公司带来了约 170 000 000 美元的直接成本。[265]

2014 年公布的相关研究结果表明，经由数据泄露获得并由网络黑市供应的数据量涉及高达 3.6 亿个帐户的证书。[266]

2.5.3 非法截获

攻击者可以截获用户之间的通信 [267]（如电子邮件）或其它形式的数据传送（当用户在网络服务器上上载数据或访问基于互联网的外部存储媒介时 [268]），以记录所交换的信息。在此方面，攻击者通常能够以任何通信基础设施（如固定线路或无线通信）以及任何国际互联网服务（如电子邮件、网络聊天或 VoIP 通信 [269]）为攻击对象。

在国际互联网基础设施提供商或国际互联网服务提供商之间进行的大多数数据传送过程都得到了良好的保护，难以截获。[270] 不过，攻击者会寻找系统中的弱点。无线技术目前越来越受欢迎，但

在过去，它被证明是脆弱的。[271] 如今，宾馆、酒店和酒吧都为客户提供通过无线接入点接入国际互联网的服务。不过，在计算机与接入点之间交换数据的信号可以在方圆 100 米的范围内被截获。[272] 想要截获数据交换过程的攻击者，可以在这一半径范围内的任何地方做到这一点，即使无线通信采用了加密技术，攻击者也能够对记录的数据进行解密。[273]

为了获取敏感信息，有些攻击者将接入点设在无线访问需求很大的地方附近 [274]（如邻近的酒吧和酒店）。他们常常以以下方式命名站点的位置，即寻求国际互联网接入点的用户更有可能选择具欺诈性的接入点。如果用户依靠接入提供商来确保其通信的安全，而不是执行其自身的安全措施，那么攻击者可以轻易地截获通信内容。

使用固定线路亦不能防止攻击者截获通信。[275] 通过电缆进行的数据传输会辐射电磁能量。[276] 如果攻击者使用恰当的设备，那么可以检测和记录这些发射，[277] 并且能够记录下用户计算机与所连接系统之间以及计算机系统内的数据传送情况。[278]

大多数国家已经开始保护对电信服务的使用，方法是对非法截获电话通话行为予以定罪。不过，鉴于基于 IP 的服务日益普及，立法者可能需要评估应当为基于 IP 的服务提供怎样的类似保护。[279]

2.5.4 数据干扰

计算机数据对于私人用户、企业和政府部门而言都是至关重要的，原因是他们都要依赖数据的完整性和可用性。[280] 无法访问数据可导致巨大的（经济）损失。攻击者可破坏数据的完整性并借助删除数据、隐瞒数据、或更改数据等方法对数据进行干扰。[281] 删除数据的一个常见例子是计算机病毒。[282] 自从计算机技术问世以来，计算机病毒就对那些没有安装适当保护措施的用户构成了威胁。[283] 自那时起，计算机病毒的数量大大增加。[284] 目前不仅病毒攻击数量加大，而且病毒（有效载荷[285]）技术和功能也发生了变化。

过去，计算机病毒通过存储设备来传播，如软盘，而如今，大多数病毒则通过国际互联网来传播，它们或者作为电子邮件的附件，或者作为用户从国际互联网上下载的文件。[286] 这些新的、有效的传播方法大大加快了病毒的感染速度，并且大大增加了受感染计算机系统的数量。据估计，计算机蠕虫 SQL Slammer [287] 在其传播过程的最初 10 分钟内，即感染了 90%的易受攻击的计算机系统。[288] 仅 2000 年一年，因计算机病毒攻击而造成的经济损失估计在 170 亿美元左右。[289] 2003 年，这一数字仍然超过 120 亿美元。[290]

大多数第一代计算机病毒或者删除信息，或者显示信息。最近，有效载荷已经变得多样化。[291] 现代计算机病毒能够安装后门，方便攻击者遥控受害者的计算机或者对文件进行加密，从而使得受害者无法访问其自身的文件，直到他们付钱买到密钥。[292]

安全公司公布的报告显示，计算机病毒及其他形式恶意软件的数量正在日益增加，且每年新出现的恶意软件字符串数多达 3 000 万个[293]。卡巴斯基公司的报告称，2013 年该公司每天均检测到逾 30 万个新的恶意文件[294]。鉴于上述数字多由销售杀毒软件的安全公司公布，因此，在确定此类数据的可靠性时，这一点无疑构成一个挑战。不过，相关发展表明，自发现第一个计算机病毒后的几十年以来，恶意软件仍是有关互联网安全的一个重大挑战。

2.5.5 系统干扰

与针对计算机数据的攻击相比，针对计算机系统的攻击同样令人担心。越来越多的企业将国际互联网服务整合到它们的生产过程中，原因是这种服务具有每天 24 小时可用以及全球可访问的优越性。[295] 如果攻击者成功阻止计算机系统顺畅运行，那么将导致受害者遭受巨大的经济损失。[296]

攻击可以通过计算机系统上的物理攻击来执行。[297] 如果攻击者能够访问计算机系统，那么他们就能够破坏硬件。对大多数刑法体系而言，远程的物理攻击并不会引发大问题，原因是它们类似有关财产破坏或损坏的典型案例。不过，对利润极高的电子商务业务而言，对计算机系统实施攻击而造成的损失，常常会比仅仅破坏计算机硬件而造成的损失大得多。[298]

对法律体系而言，最大的挑战是基于互联网的诡计。这些针对计算机系统的远程攻击的例子包括：计算机蠕虫[299] 和拒绝服务（DoS）攻击。[300]

计算机蠕虫 [301] 是恶意软件的一个子群（与计算机病毒一样）。计算机蠕虫是一种自我复制的计算机程序，它们通过启动多个数据传送过程来对网络造成损害。它们可以通过以下方式影响计算机系统的顺畅运行：使用系统资源在国际互联网上对自身进行复制；产生网络流量，使某些服务（如网站）不再可用。

尽管计算机蠕虫的目标通常是影响整个网络，而不是针对某些特定的计算机系统，但拒绝服务（DoS）攻击的目标是一些特定的计算机系统。拒绝服务攻击使目标用户无法使用计算机资源。[302] 通过发出比计算机系统能处理的请求更多的请求来攻击某个目标计算机系统，攻击者可以阻止用户访问计算机系统、查看电子邮件、阅读新闻、预订航班或者下载文件。2000 年，在短时间内，对一些知名的公司，如美国有线新闻网（CNN）、易趣（eBay）和亚马逊（Amazon）[303]，发动了若干次拒绝服务攻击。据报道，2009 年亦针对美国和韩国的政府和商业网站发起过类似攻击。[304] 结果是，有些服务在数小时内甚至几天内无法使用。[305]

对拒绝服务攻击和计算机蠕虫攻击进行起诉，对大多数刑法体系提出了严峻挑战，原因是这些攻击可能不会对计算机系统造成任何物理影响。除了对基于互联网的攻击需要进行定罪的基本需求外，[306] 对防止和起诉针对关键基础设施的攻击是否需要一种独立的法律方式的问题，目前正在讨论之中。

尽管技术防范工具和缓解战略一直在发展，但拒绝服务攻击仍是企业和政府机构面临的一个挑战。有研究表明，此类攻击的危险性和相关成本正在与日俱增。[307]

2.6 内容相关的违法行为

参考书目（节选）： *Akdeniz*, Governance of Hate Speech on the Internet in Europe, in Governing the Internet Freedom and Regulation in the OSCE Region; *Carr*, Child Abuse, Child Pornography and the Internet, 2004; *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144 *et seq.*; *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Healy*, Child Pornography: An International Perspective, 2004; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001; *Lanning*, Child Molesters: A Behavioral Analysis, 2001; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*; *Siebert*, Protecting Minors on the Internet: An Example from Germany, in Governing the Internet Freedom and Regulation in the OSCE Region, page 150, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/.

这一类别涵盖了那些被认为是非法的内容，包括儿童色情、排外资料或者与宗教符号有关的侮辱。[308]应对这一类别违反行为的法律手段的制定更大程度上受国家级措施的影响，需要考虑基本的文化和法律原则。对非法内容，不同社会之间的价值体系和法律体系会存在众多不同之处。在许多欧洲国家，散发排外资料是非法的，[309] 但在美国，[310] 却受到该国言论自由原则的保护。[311] 在许多阿拉伯国家，对神圣的先知使用不敬的言论是犯罪行为，但在一些欧洲国家却不是这样。[312]

将非法内容定罪的法律途径不应干涉表达自由的权利。例如，《有关国家安全、表达自由及获取资料的约翰内斯堡原则》的第 1 (b) 条原则定义了自由表达的权利。[313] 但是，第 1 (c) 条原则做出了澄清，即自由表达的权利可能会受到限制。尽管不能因此排除将非法内容入罪的做法，但必须加以严格限制。尤其在诽谤定罪方面需要讨论这类限制。[314] “2008 年联合国有关意见和表达自由的特别报告人联合声明”等文件指出，不应将提供通信以及颂扬或推广恐怖主义或极端主义等模糊概念定为犯罪行为。[315]

这些法律挑战是复杂的，原因是在某个国家中计算机用户可用的信息，几乎可以被全世界任何地方的人访问到。[316]如果“攻击者”制造了在某些国家被视为非法的内容，但他身处这些国家之外，那么很难、甚至不可能起诉“攻击者”。[317]

关于资料的内容，以及特定行为应定位为何种程度的罪行，各国间很难达成一致。不同的国家观点，以及难以起诉在调查国之外的地方所犯的违法行为，已促使对国际互联网上的某些类型内容进行阻断。有些国家已就防止访问含有非法内容、主机设在国外的网站达成一致，这样，这些国家就可实施严格的法律，阻断对网站的访问，并对内容进行过滤。[318]

内容过滤系统可采用各种各样的方法。一种解决方案要求访问提供商安装对即将访问的网站进行分析的程序，并阻止对黑名单上网站的访问。[319]另一种解决方案是在用户计算机上安装过滤软件（对于那些希望控制子女们网上浏览内容的父母，这是一种有用的方法，对于图书馆和公共国际互联网终端也是如此）。[320]

尝试控制国际互联网上的内容不限于那些被广泛认为是非法的内容类型。一些国家使用过滤技术来限制对涉及政治主题的网站的访问。开放网络倡议[321]报告说，当前约有 20 个国家实施这种审查制度。[322]

2.6.1 色情资料（不包括儿童色情）

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

- 媒介交换（如图片、视频、实况转播等），而无需进行高成本的运输；[323]
- 在世界范围内[324]访问，客户数量可以比零售店的顾客数量多得多；
- 国际互联网常常被视为一种匿名媒介（常常是错误的[325]）– 鉴于当前主流的社会观念，这是色情内容消费者欣赏的一个方面。

最近的研究已确定，任何时候，国际互联网上都有 420 万个色情网站可供访问。[326]除这些网站外，色情资料还可以通过文件共享系统[327]和即时消息系统进行传播。

不同国家对色情与淫秽资料的定罪程度各不相同。有些国家允许成年人交流色情资料，并仅对未成年人访问这类资料的情形予以定罪[328]，旨在保护未成年人。[329]研究表明，儿童接触色情内容会对其成长产生负面影响。[330]为遵守这些法律，一些国家研发了“成人验证系统”。[331]另一些国家则

将所有有关色情资料的交流定为犯罪行为，即使是成年人也不例外，[332]而不专门针对特定群体（如未成年人）。

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

国家主权原则通常不允许某个国家在未经当地主管部门许可的条件下，到他国领土范围内开展调查。[333]即使当主管部门寻求违法网站托管服务国的支持时，案件的成功调查和刑事制裁也可能受到“双重犯罪”原则的阻碍。[334]为防止人们访问色情内容，制定了严格法律的国家也常常局限于防止（如采用过滤技术[335]）对某些网站的访问。[336]

2.6.2 儿童色情

国际互联网已成为儿童色情传播的主要渠道。在 20 世纪 70 年代和 80 年代，从事儿童色情物品交换的违法者曾面临严重威胁。[337] 当时，商业性儿童色情市场主要集中于欧洲和美国，[338] 并且儿童色情资料是本地制作的，价格昂贵且难以获取。[339] 购买或出售儿童色情物品的途径曾存在大量风险，而如今这种风险已 – 或至少在某种程度上 – 不复存在。过去，生产商不具备冲洗照片和胶卷的能力。[340] 他们依赖于相关企业提供的服务，这就增加了执法人员根据处理冲洗业务的公司提供的报告来确定儿童色情物品的机会。[341]摄像机的问世首次改变了这一情况。[342] 但是风险不仅涉及制作方面。对于违法者而言，获取儿童色情物品同样也充满了风险。订购通过回复报纸中的广告进行。[343] 卖方和收集人之间的沟通手段以及市场本身规模都非常有限。[344] 直到 20 世纪 90 年代中期之前，儿童色情物品主要通过邮寄服务运输，并且成功的调查工作查处了大量违法者。[345] 专家认为，当时的执法工作能够应对所面临的各种挑战。[346]

随着基于国际互联网的数据交换应用的出现，情况发生了急剧转变。过去，执法工作处理的是模拟资料，而今天发现的绝大多数资料都是数字资料。[347] 自 20 世纪 90 年代以来，违法者已越来越多地利用网络服务来传播这类资料。[348]目前已普遍承认这种转变对儿童色情案件的调查工作所造成的问题。[349] 如今，国际互联网是交易一般色情物品[350] 和儿童色情物品的主要渠道。[351]

可以确定多个从模拟传播转向数字传播的原因。国际互联网使得技术技能欠缺的用户以为其他用户无法发现他们的行为。如果违法者不使用匿名通信技术，则这种印象是错误的。但是，在儿童色情物品在线交换方面，使用先进的匿名通信手段可以阻碍确定违法者的工作，这是一项值得关注的问题。[352] 此外，用于制作和交易儿童色情物品的技术设备和服务（例如录制设备和主机托管服务）的价格下降为这种发展提供了支持。[353] 由于网站和国际互联网服务面向大约 20 亿互联网用户开放，潜在客户的数量亦得到扩大。[354] 有人担心，访问更加容易的事实会吸引原本不会冒着被查获风险的人们试图在国际互联网以外获取儿童色情物品。[355] 随着从模拟向数字媒体的转变，报道称，通过调查发现的儿童色情图片数量日益增加。[356] 可能为这种发展提供支持的另一方面是，数字信息的复制一般不会降低质量。[357] 过去，希望复制资料并进行交易的儿童色情物品消费者会因复制造成的质量损失而受到阻碍，而现在的下载文件可以作为进一步复制的源文件。这种发展的后果之一是，即使最先制作资料的违法者被拘捕，并且涉案文件被没收，但是一旦这些文件已通过国际互联网进行交易，则很难将其“删除”。[358]

与各国对成人色情的不同观点相反，全世界都对涉及儿童色情的行为予以谴责，并将涉及儿童色情的违法行为广泛地视为犯罪行为。[359] 一些国际组织致力于与在线儿童色情作斗争，[360] 这方面的一些国际法律倡议包括：1989 年《联合国关于儿童权利的公约》；[361] 2003 年《欧洲理事会关于与儿童性侵犯和儿童色情作斗争的框架决定》；[362] 以及 2007 年《欧洲理事会关于保护儿童免受性侵犯和性虐待的公约》，等等。[363]

令人遗憾的是，这些旨在控制网络传播色情的倡议并没有阻止违法者通过国际互联网来传递和交换儿童色情资料。[364] 带宽的增加还为此类电影和图片资料的交换提供了支持。

对涉及儿童色情的违法者行为进行的研究表明，在因涉嫌与国际互联网有关的儿童色情犯罪而逮捕的人中，15%的人在其计算机中存有 1000 多张儿童色情图片；80%的人在其计算机中存有 6～12 岁儿童的色情图片；[365] 19%的人存有年龄在 3 岁以下儿童的色情图片；[366] 21%的人存有描绘暴虐的图片。[367]

销售儿童色情有大利可图，[368] 收集者愿意为描述儿童色情内容的电影和图片支付大笔费用。[369] 搜索引擎可以迅速找到此类资料。[370] 大部分资料是在有密码保护的、封闭的论坛中进行交易的，此类论坛对普通用户和执法机构而言是难以访问的。因此，暗中进行侦查是与儿童色情犯罪活动进行斗争的关键所在。[371]

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

1 使用虚拟货币和匿名支付手段 [372]

现金支付使购买者能不暴露其身份而购得物品，因此，现金支付在许多犯罪行业中占有主导地位。对匿名支付的需求使得虚拟支付系统和实现匿名支付的虚拟货币应运而生。[373] 虚拟货币无需身份和验证，防止了执法机构对流向违法者的资金流进行跟踪。最近，对儿童色情犯罪活动的大量调查成功地利用了在支付时留下的踪迹来鉴别违法者。[374] 不过，当违法者使用匿名支付时，则难以对其进行跟踪。[375] 如果犯罪分子使用匿名货币，则限制了执法机构通过跟踪资金转账确定犯罪嫌疑人的能力[376] – 例如在与商业性儿童色情内容有关的案件中。[377]

2 使用加密技术[378]

越来越多的违法者对其消息进行加密。执法机构注意到，违法者使用加密技术来保护存储在其硬盘上的信息，[379]这严重阻碍了犯罪调查。[380]

除了对涉及儿童色情的犯罪行为进行广泛定罪外，目前正在讨论其他一些方法，如履行国际互联网服务必须注册用户的义务，或者阻止或过滤对涉及儿童色情内容的网站的访问等。[381]

2.6.3 种族主义、仇恨言论、鼓吹暴力

激进团体使用国际互联网等大众传播系统来开展宣传活动。[382] 最近，提供种族主义内容和仇恨言论的网站数量已经在增长[383] – 2005 年的一份研究表明，在 2004 年至 2005 年间，鼓吹种族仇恨、暴力和排外主义的网页数量增加了 25% 。[384] 2006 年，在国际互联网上存在 6000 多个类似的网站。[385]

国际互联网的传播为违法者提供了若干优势，包括更低的传播成本、无需专业设备以及在全球范围内散布。鼓吹仇恨网站的例子包括介绍如何制造炸弹的网站。[386] 除了进行宣传活动之外，国际互联网还被用来出售某些产品，如与纳粹有关的物品，包括带纳粹符号的旗帜、制服和书籍，这些东西都可以在拍卖平台和专门的互联网商店中轻易地得到。[387] 国际互联网还用来发送电子邮件、新闻简报，以及通过一些受欢迎的网站（如 YouTube）传播视频片段和电视节目。

并非所有国家都对这些违法行为定罪。[388]在有些国家，此类内容可能得到言论自由原则的保护。[389]对某些主题言论自由原则运用到何种程度，各国之间存在不同意见，这常常妨碍了国际调查。这方面法律冲突的一个例子涉及国际互联网服务提供商雅虎。2001 年，法国的一个法庭命令雅虎（位于美国）阻止法国用户访问与纳粹有关的内容。[390] 根据美国宪法第一修正案，销售此类资料

并不违反美国法律。根据第一修正案，美国的一个法庭宣布法国的命令无法对位于美国的雅虎执行。[391]

在起草《欧盟理事会关于网络犯罪的公约》时，各国之间对这些问题的分歧表现明显。《公约》寻求协调与网络犯罪有关的法律，以确保国际调查不因法律冲突而受阻。[392] 在讨论关于如何就散布排外主义资料的行为定罪时，并非参加谈判的所有各方都一致同意，因此，这整个主题排除在了《公约》之外，取而代之的是在一个单独的《第一协议》中进行了论述。[393] 否则，有些国家（包括美国在内）可能不会签署《公约》。

2.6.4 冒犯宗教的行为

越来越多的网站 [394] 介绍一些其他国家可能视为冒犯宗教的行为内容，如反宗教的书面声明。[395]尽管有些资料记录了客观的事实与趋势（如欧洲参加教堂活动的人数日益减少），但在一些管辖区域中，这类信息也可能被视为非法。另一些例子包括诽谤宗教或者出版漫画。

国际互联网为那些希望引起争论或对某一主题进行批判的人提供了优势 — 人们可以留下评论、张贴内容或者撰写文章，而不必暴露其身份。许多辩论团体都是基于言论自由原则的。[396]言论自由原则也是国际互联网成功背后的一个主要推动因素，门户网站是专用于用户自己制作的内容的。[397]虽然保护这一原则至关重要，但即使在最自由的国家，言论自由原则的适用也受到各种条件和法律的控制。

关于非法内容的不同法律标准，体现了在管理这些内容中所面临的挑战。尽管在那些奉行言论自由原则的国家可以发表某些内容，但在另一些管制更严格的国家，它可能会受到指责和控告。2005 年的“漫画争议”就显示了各国法律冲突的可能性。一家丹麦报纸《日德兰邮报》发表的十二幅由编辑制作的漫画，引发了穆斯林世界的广泛抗议。[398]

谈到非法内容，在某些国家，提供某些信息或资料的可用性是一种犯罪行为。国与国之间对不同宗教信仰和宗教符号的保护政策各不相同。有些国家对“圣洁先知”[399]使用不敬言论或者玷污《可兰经》[400]的行为认为有罪，而另一些国家则可能采取更为自由的方法，可能不对此类行为进行定罪。

2.6.5 非法赌博与在线游戏

国际互联网游戏和网络赌博是国际互联网世界里增长最快的领域之一。[401]在线游戏“Second Life”的研发商林登（Linden）实验室 [402]报告说，该游戏目前大约有 1000 万注册用户。[403]有报告显示，一些此类游戏已被用来实施犯罪，包括[404]交换和展示儿童色情内容、[405]欺诈、[406]虚拟在线赌场中的赌博[407]以及诽谤（例如，留下诽谤性或损害他人名誉的消息）。

有人估计，从 2001 年到 2010 年的 10 年间，预计国际互联网在线赌博的年均收入从 31 亿美元增长到了 240 亿美元 [408]（尽管与传统赌博业的收入相比，这些估计值仍然相对较小 [409]）。2015 年这方面的估算收入为 280 亿美元。[410]

各国对国际互联网上和国际互联网外的赌博的管制各不相同 [411] – 这正是违法者、合法企业以及各个赌场加以充分利用的一个漏洞。不同管制的效应在澳门最为明显。自从 1999 年澳门从葡萄牙回归中国后，澳门已经成为全世界最大的赌博目的地之一。2006 年，澳门赌博业估计的年收入为 68 亿美元，取代了拉斯维加斯的龙头老大位置（拉斯维加斯的赌博业年收入为 66 亿美元）。[412]澳门的成功源于中国法律禁止赌博这一事实，[413]每年有成千上万的大陆居民前往澳门赌博。

国际互联网使人们可以绕过对赌博的限制。[414]在线赌场在网上随处可见，而大多数的托管服务器都设在对国际互联网赌博不加限制或者法律宽松的国家。用户可以在线开设账号，转移资金并且玩这种运气游戏。[415]在线赌场还可以用于洗钱和资助恐怖主义等活动。[416]如果违法者在不保存记录的下注阶段使用在线赌场，或者在没有针对洗钱犯罪进行过立法的国家中使用在线赌场，那么执法机构将难以确定资金的源头

对于那些限制赌博的国家，难以控制人们对在线赌场的使用或参与在线赌博活动。国际互联网破坏了一些国家禁止公民参与在线赌博的法律限制。[417] 一些国家试图通过立法防止国民参与在线赌博：[418]一个著名的例子是，美国于 2006 年出台的禁止国际互联网赌博法案，它试图通过对那些涉及非法赌博结算的金融服务提供商进行起诉来限制非法的在线赌博。[419]

2.6.6 诽谤与虚假信息

国际互联网可用来散布虚假信息，这与用它来发布真实信息一样容易。[420]网站可以发布虚假的或诽谤性的信息，尤其是在论坛和聊天室中，在这些地方，用户可以不经过版主的验证就可发布消息。[421]越来越多的未成年人使用网上论坛和社交网站，而在这些地方也可以发布类似的虚假或诽谤信息。[422] 犯罪行为[423]包括（例如）发布激情照片或者发布关于性行为的虚假信息。[424]

在大多数情况下，违法者利用以下事实来实施犯罪活动，即提供商提供廉价或免费发布消息的服务，通常无需发布者身份证明或者不必验证身份。[425]这使得对违法者的身份识别变得更加复杂。此外，论坛版主对其中发布的内容不做规定，或者只有很少的规定。但这些优势并没有阻碍到一些有价值项目的发展，如由用户生成的在线百科全书 — 维基（Wikipedia）[426]，该项目对发布的内容存在严格的管制程序。不过，违法者也可以使用同样的技术来发布虚假信息（例如，发布关于竞争者的虚假信息）[427]或泄漏秘密信息（例如，发布国家机密或者敏感的商业情报）。

重要的是强调虚假或欺骗信息所带来的日益严重的威胁。诽谤可以在很大程度上严重毁坏受害者的名誉和声望，原因是全球的用户都可以访问到在线信息。从信息在国际互联网上发布的那一刻起，作者往往就失去了对它的控制。即使在信息发布后不久就更正或删去，它也可能已被复制（“镜像”），并被那些不愿撤销或删除它的人得到。在这种情况下，信息在国际互联网上仍然是可用的，即使最初的发布者已经删除或者进行更正。[428]这方面的例子包括“失控的电子邮件”，数以百万计的用户可以接收到关于个人或组织的色情的、欺骗的或虚假的电子邮件，而它们对名誉的伤害也许永远无法消除，尽管事实与最初发出的电子邮件完全相反。因此，需要在言论自由[429]与保护因言论自由而可能遭到伤害的受害者之间保持良好的平衡。[430]

2.6.7 垃圾信息与相关威胁

“垃圾邮件”指的是发送主动提供的大量消息。[431]尽管存在各种各样的垃圾信息，但最为常见的是垃圾邮件。违法者向用户发出数百万封电子邮件，常常包含产品和服务的广告，但也经常带有一些恶意软件。自从 1978 年第一封垃圾邮件发出之日起，[432]垃圾邮件便呈现急剧增长的态势。[433]如今，根据电子邮件提供商组织的报告，在所有电子邮件中，多达 85%～90%是垃圾邮件。[434] 2007 年，垃圾邮件主要来自：美国（占记录总数的 19.6%）；中华人民共和国（占记录总数的 8.4 %）以及韩国（占记录总数的 6.5%）。[435] 六年以后，垃圾邮件的前三大来源国仍保持不变，分别是：中华人民共和国（22.97%）、美国（占记录总数的 17.6%）和韩国（12.67%）。[436]

大多数电子邮件提供商通过安装反垃圾邮件过滤技术，对垃圾邮件数量猛增的态势作出了反应。这种技术使用关键字过滤器或者垃圾邮件发送者 IP 地址黑名单来识别垃圾邮件。[437]尽管过滤技术仍在继续研发之中，但垃圾邮件发送者已经围绕这些系统在寻找应对之策 — 例如，避开过滤技

术可能发现的关键字。垃圾邮件发送者已经找到许多办法来描述“伟哥”这种最常出现在垃圾邮件中的产品，方法是在电子邮件中不使用其商标名称。[438]

成功检测垃圾邮件取决于垃圾邮件传播方式是否改变。许多攻击者不是使用单个邮件服务器来发送垃圾邮件（由于其源头数量有限，[439]这在技术上更易于检测到垃圾邮件提供商），而是运用僵尸网络[440]来分发主动提供的电子邮件。通过使用基于成千上万个计算机系统的僵尸网络，[441]每台计算机可能只发送几百封电子邮件。这使电子邮件提供商更难借助分析邮件发送者信息的方法来识别垃圾邮件，也使执法机构更难追踪犯罪者。

由于发送数十亿封垃圾邮件的成本很低，因此垃圾邮件是十分有利可图的 — 如果使用僵尸网络，那么成本更低。[442]有些专家建议，在与垃圾邮件作斗争的过程中，唯一真正的解决方案是提高发送者的邮件发送成本。[443] 2007 年公布的一份报告对垃圾邮件的成本与利润进行了分析。根据分析结果，发送 2000 万封垃圾邮件的成本约为 500 美元。[444]由于发送者成本很低，因此发送垃圾邮件的利润相当高，尤其当发送者能够发送数十亿封电子邮件时。荷兰的一位垃圾邮件发送者指出，通过发送至少 90 亿封垃圾电子邮件，获得了大约 50000 美元的利润。[445]

2005 年，经济合作与发展组织公布了一份报告，对垃圾邮件对发展中国家的影响进行了分析。[446]发展中国家常常表达这样的观点：它们国家中的国际互联网用户更多地受到垃圾邮件和国际互联网滥用的影响。垃圾邮件在发展中国家里是一个严重问题，原因是在发展中国家，带宽和国际互联网接入资源比在工业化国家更加稀缺、昂贵。[447]在那些国际互联网资源更稀缺、更昂贵的国家，垃圾邮件占用了宝贵的时间与资源。

2.6.8 勒索

勒索一般不被认为是典型的网络犯罪，而是被当成一种传统犯罪形式。不过，ICT 用途的兴起已催生了通常被称为“网络勒索”的攻击。[448]近年来，无论大公司还是小型初创公司均曾成为此类攻击的目标。[449]与传统犯罪手段不同，违法者对 ICT 所提供若干优势的利用正在方兴未艾。除使用匿名通信技术实施犯罪以外，越来越多的犯罪分子开始使用虚拟货币（而非现金电汇）进行支付。[450]研究表明，企业对勒索隐患的认识仍然不足。[451]

勒索的一个更自动化形式是所谓的“勒索软件”—此类恶意软件首先感染受害者的计算机系统，然后将系统锁定，并提示受害者支付赎金，以解锁计算机。各方对此类软件的关注正在与日俱增。[452]为了更有说服力，罪犯常常佯称执法者发现计算机用户进行了非法活动，并因此关闭了计算机系统。[453]

2.6.9 其他形式的非法内容

国际互联网不仅用于直接攻击，而且还可作为一个论坛，进行教唆和煽动犯罪[454]、非法出售产品以及为非法行为提供信息和指导（例如，指导如何制造爆炸物）等非法活动。

许多国家对某些产品的交易实施严格的管理。不同国家运用不同的国家规定和贸易限制来对各种产品进行严格的监管，如军用装备。[455]药品也面临同样的情形 — 在某些国家不受限制即可获得的药品，在另一些国家可能需要处方。[456]跨境贸易使得难以确保在领土内对某些产品的获取实施严格限制。[457] 鉴于国际互联网的广泛普及，这一问题变得更为严重了。在那些不设限制的国家中经营的互联网商店，可以向其他设有严格限制的国家的客户出售产品，这就破坏了这些限制。

在国际互联网问世之前，大多数的人难以接触到如何制造武器之类的指南。尽管也可以获得一些必要的信息（例如，在涉及爆炸物方面化学的书籍中），但这相当费时。如今，国际互联网上就有关于如何制造爆炸物的指南，[458]而且可以轻易地获得此类信息，这增大了攻击的可能性。

2.7 与版权和商标有关的违法行为

参考书目（节选）： Androutsellis-Theotokis/Spinellis, A Survey of Peer-to-Peer Content Distribution Technologies, 2004, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; Bakken, Unauthorized use of Another's Trademark on the Internet, UCLA Journal of Law and Technology Vol. 7, Issue 1; Baesler, Technological Protection Measures in the United States, the European Union and Germany: How much fair use do we need in the digital world, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a13-Baesler.pdf; Clarke/Sandberg/Wiley/Hong, Freenet: a distributed anonymous information storage and retrieval system, 2001; Cunard/Hill/Barlas, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; Fischer, The 21st Century Internet: A Digital Copy Machine: Copyright Analysis, Issues, and Possibilities, Virginia Journal of Law and Technology, Vol. 7, 2002; Johnson/McGuire/Willey, Why File-Sharing Networks Are Dangerous, 2007, available at: http://oversight.house.gov/documents/20070724140635.pdf; Lohmann, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/_20030401_drm_skeptics_view.pdf; Penn, Copyright Law: Intellectual Property Protection in Cyberspace, Journal of Technology Law and Policy, Vol. 7, Issue 2; Rayburn, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001; Schoder/Fischbach/Schmitt, Core Concepts in Peer-to-Peer Networking, 2005, available at: www.idea-group.com/downloads/excerpts/Subramanian01.pdf; Sifferd, The Peer-to-Peer Revolution: A Post-Napster Analysis of the Rapidly Developing File-Sharing Technology, Vanderbilt Journal of Entertainment Law & Practice, 2002, 4, 93.

国际互联网至关重要的功能之一是传播信息。各家公司使用国际互联网来传播关于其产品与服务的信息。在盗版方面，成功的公司在国际互联网上可能面临的问题，比那些网络之外存在的问题有过之而无不及。它们的品牌形象和公司设计可能用于推销仿造的产品，而仿造者复制公司的标识，仿造其产品，并试图在与该公司相关的域上注册。直接通过国际互联网发售其产品的公司[459]可能面临与侵犯版权有关的法律问题。它们的产品可以被下载、复制和发售。

2.7.1 与版权有关的违法行为

利用数模转换，[460] 数字化[461]使得娱乐行业为 DVD 中的电影增加了额外的特点与服务，包括语言、字幕、预告片以及额外赠送的资料。CD 和 DVD 已被证明能比录音带和录像带保存更长的时间。[462]

数字化也为新的版权侵犯行为打开了方便之门。当前侵犯版权的基础是快速而准确地复制。在数字化之前，复制一盘录音带或录像带总会导致一定程度的质量下降。如今，复制数字音像制品几乎不会造成质量的下降，因此，也能够从任何拷贝再次复制。最常见的版权侵犯行为包括在文件共享系统中或通过共享主机服务共享受版权保护的歌曲、文件和软件[463]，以及规避数字版权管理（DRM）系统。[464]

文件共享系统是基于点对点[465]的网络服务，它使用户能够共享文件，[466] 常常可以与数百万个其他用户实现共享。[467]在安装文件共享软件后，用户可以选择一些文件来共享，并使用软件来搜索其他用户提供的文件，这些文件可从数百个出处下载。在文件共享系统问世之前，人们需要复制录音带和录像带，然后才能进行交换，文件共享系统则允许更多的用户进行拷贝交换。

点对点（P2P）技术在国际互联网中起着至关重要的作用。2007 年，超过一半的用户国际互联网通信流量是由点对点网络产生的。[468]用户数量一直在增长 — 经济合作与发展组织公布的一份报告估计，30%左右的法国国际互联网用户在文件共享系统中下载过音乐或文件，[469] 而这一组织中的其他国家也呈现类似的趋势。[470]文件共享系统可用来交换任何类型的计算机数据，包括音乐、电影

和软件。[471]过去，文件交换系统主要用来交换音乐，但如今，视频资料的交换变得愈来愈重要了。[472]

用于文件共享服务的技术极为先进，能够在短时间内交换大型文件。[473]第一代文件共享系统依靠一台中央服务器，使得执法机构能够针对 Napster 网络中的非法文件共享行为采取行动。[474]与第一代系统（尤其是著名的服务 Napster）不同，第二代文件共享系统不再以中央服务器为基础（中央服务器用于提供用户间可用的文件列表）。[475]第二代文件共享系统的分散管理概念，使得更难以防止它们运行。不过，由于采用直接通信，因此，通过用户的 IP 地址，还是有可能跟踪到网络用户的。[476]执法机构已经在调查文件共享系统中的版权侵权问题上取得一些成功。最近版本的文件共享系统能够实现多种形式的匿名通信，这将使版权侵权问题的调查变得更加困难。[477]

文件共享技术不仅可被普通用户和犯罪分子使用，普通的企业也可以使用。[478] 并非在文件共享系统中交换的所有文件都侵犯版权。合法使用文件共享系统的例子包括授权拷贝的交换或者公共域中的艺术作品。[479]

尽管这样，文件共享系统的使用仍然对娱乐行业提出了挑战。[480] 目前尚不明确，CD/DVD 以及电影票销量的下滑究竟在多大程度上应归咎于文件共享系统中电影拷贝的交换。研究确定已有数百万个文件共享用户 [481]以及数十亿个已被下载的文件。[482] 常常是在电影在电影院正式上映之前，电影拷贝就已经出现在文件共享系统中，[483] 这损害了版权持有者的利益。匿名文件共享系统的最新发展将使版权持有者的反盗版工作更难进行，也令执法机构更难执法。[484]

通过实施一种专用于防止用户制造 CD 和 DVD 拷贝的技术，如内容加扰系统（CSS） [485] — 一种旨在防止 DVD 上内容被拷贝的加密技术，[486] 娱乐业已经对盗版行为作出了反应。这种技术是新商业模式一个不可或缺的因素，旨在更加准确地向用户赋予访问权限。数字版权管理（DRM）[487] 描述了有关技术的实施情况，它们允许版权持有者限制他人对数字媒体的使用，客户只能购买有限的权限（例如，只能在一次集会上演唱某首歌曲的权限）。数字版权管理使得新商业模式的实施成为可能，它可更加准确地体现版权持有者和用户的权益，有望扭转利润下滑的趋势。

这些技术最大的困难之一是，侵权者可以绕过版权保护技术。[488] 侵权者已经开发出一些软件工具，使软件工具用户能够使受版权保护的文件在国际互联网上可用，[489] 且是免费的，或者价格低廉。一旦从文件中移去数字版权管理（DRM）保护措施，拷贝就可以不受限制地被复制和使用。

版权保护的内容不只限于歌曲和电影。有些电视台（尤其是付费电视频道）对其节目进行加密，以确保只有付费用户才能收看到节目。尽管此类保护技术十分先进，但违法者仍成功地伪造了用于访问控制的硬件，或者使用软件工具破解了密码。[490]

没有软件工具，普通用户不太可能实施违法行为。对侵犯版权行为的定罪的讨论，不仅关注文件共享系统和绕过技术保护，而且关注生产、销售和拥有旨在使用户能够实施版权侵权活动的“非法设备”或工具。[491]

2.7.2 与商标有关的违法行为

侵犯商标类似于侵犯版权，也是全球贸易中一个广为人知的问题。涉及商标的侵犯行为已经转向网络空间，根据不同国家的刑法，定罪的轻重也各不相同。[492] 最严重的违法行为包括在犯罪活动中使用商标误导用户以及与域名有关的违法行为。

一家公司的良好声誉常常直接和其商标相关联。违法者在许多活动中使用品牌名称和商标进行欺诈，包括“网络钓鱼”，[493] 在此类违法行为中，违法者向国际互联网用户发出数百万封电子邮件，这些邮件与合法公司发出的电子邮件相似，例如，都包括其商标。[494]

与商标侵权有关的另一个问题是与域名有关的违法行为，[495] 如域名抢注，[496] 是指注册一个与某一产品或某家公司的商标相同或相似的域名的非法行为。[497] 在大多数情况下，违法者寻求向该公司高价出售这一域名，[498] 或者利用它来销售产品或服务，借助用户对该商标信以为真的连接来误导他们。[499] 另一种与域名有关的违法行为是“域名劫持”或者注册偶然终止的域名。[500]

2.8 与计算机有关的违法行为

参考书目（节选）： *Bywell/Oppenheim*, Fraud on Internet Auctions, Aslib Proceedings, 53 (7), page 265 *et seq.*; *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf; *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, 2005; *Gercke*, Internet-related Identity Theft, 2007; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270; *Mitchison/Wilikens/Breitenbach/Urry/Poresi,* Identity Theft – A discussion paper, 2004; *Paget*, Identity Theft – McAfee White Paper, page 10, 2007; *Reich*, Advance Fee Fraud Scams in-country and across borders, Cybercrime & Security, IF-1; *Sieber*, Council of Europe Organised Crime Report 2004; *Smith/Holmes/Kaufmann*, Nigerian Advance Fee Fraud, Trends & Issues in Crime and Criminal Justice, No. 121; *Snyder*, Online Auction Fraud: Are the Auction Houses Doing All They Should or Could to Stop Online Fraud, Federal Communications Law Journal, 52 (2), page 453 *et seq.*

这一类别涵盖大量的违法行为，它们需要借助计算机系统来实施。与之前的类别不同，这些众多的违法行为通常不会受到法律原则的严格保护，它们包括：与计算机有关的欺骗；与计算机有关的伪造、网络钓鱼和身份盗用；以及设备误用。

2.8.1 欺诈和与计算机有关的欺诈

与计算机有关的欺诈是国际互联网上最常见的犯罪之一，[501] 原因是它使违法者能够使用自动操作工具[502]和软件工具来掩盖作案者的身份。

自动操作工具可使违法者从大量的小金额违法行为中获取巨额利润。[503]违法者使用的一种战略是确保每个受害者遭受的经济损失都低于某个特定界限。由于损失“很小”，受害者不太可能耗费时间和精力来报告和调查此类罪行。[504] 此类骗局的一个例子是尼日利亚的预付金欺诈案。[505]

尽管这些违法行为都是使用计算机技术来实施的，但大多数刑法体系并未将其归类为与计算机有关的违法行为，而是将其归类为普通欺诈。[506] 与计算机有关的欺诈与普通欺诈之间的主要区别在于欺诈的对象。如果违法者试图影响一个人，那么其行为通常被视为欺诈。如果违法者以计算机或数据处理系统为目标，那么其行为通常被视为与计算机有关的欺诈。那些涵盖欺诈行为但尚纳入出于欺诈目的而操纵计算机系统的违法行为的刑法体系，常常也会对上述行为进行起诉。最常见的欺诈骗局包括：在线拍卖欺诈和预付金欺诈。

在线拍卖欺诈[507]

在线拍卖目前是最受欢迎的电子商务服务之一。早在 2006 年，通过易趣（eBay）销售的商品价值即已超过 200 亿美元，这令易趣（eBay）成为世界上最大的在线拍卖市场。[508] 购买者可以从世界各地通过国际互联网访问各种不同的或者专门的利基商品。销售者乐于面对全球受众，刺激需求、提升价格。

通过拍卖平台实施犯罪的违法者，可以充分利用买方与卖方之间不存在面对面签订合同的机会。[509] 由于难以区别真正的用户与违法者，因此导致拍卖欺诈成为最常见的网络犯罪之一。[510] 最常见的两种欺诈方法 [511] 包括用一种实际并不存在的商品进行销售，并要求买方在发货之前付款[512]；以及买下商品并要求发货，但不打算付款。

在应对这种违法活动时，拍卖提供商开发了一种保护系统，如反馈/评价系统。在每笔拍卖交易后，买方和卖方留下供其他用户使用的反馈意见，[513]作为一种关于买方/卖方可靠性的中性信息。在这种情况下，“信誉就是一切”，如果没有足够数量的积极评价，违法者难以说服他要欺诈的对象为并不存在的商品付款，或者相反地，在没有预先收到付款的情况下发货。不过，作案者也为此想出了对策，通过使用第三方的账号，来绕过这一保护措施。[514] 在这一骗局中称为“账号接管”，[515] 违法者设法掌握合法用户的用户名和密码，以便以欺诈手段购买或销售商品，使执法机构更难确定违法者的身份。

预付金欺诈[516]

在预付金欺诈中，违法者发出电子邮件，请求接收者帮助向第三方转移大笔资金，并承诺，如果接收者同意使用其个人账号来转账，那么将给其一定比例的“回扣”。[517] 然后，违法者要求邮件接收者转移一笔小额资金，以验证其银行账号数据（基于一种类似于碰碰运气的情形 — 接收到邮件的人也许愿意遭受小而肯定的损失，来换取大而不可能的收入），或者要求他们直接发送银行账号数据。一旦受害者转移了资金，他们将再也联系不上违法者。如果他们向违法者发送了银行账号信息，那么后者可能利用这些信息来进行其他欺诈活动。有证据表明，数以千计的受害者对此类电子邮件进行了回复。[518] 当前的研究表明，尽管政府部门进行了各种各样的宣传，也采取了一些举措来遏制这种犯罪，但预付金欺诈案件的数量仍在不断增长 — 不仅仅是受害者的数量在增加，总的损失数额也在增加。[519]

2.8.2 与计算机有关的伪造

与计算机有关的伪造指的是对数字文件的操纵。[520] 例如，可通过创建一个看起来像来自可靠机构的文件，篡改电子图像（例如，在法庭上用作证据的图片）或者更改文本文件等方法实施犯罪。

伪造电子邮件是“网络钓鱼”骗局的重要手段之一，这对全世界的执法机构都是一个严峻的挑战。[521]“网络钓鱼”力图让欺诈对象泄露个人/秘密信息。[522] 通常，违法者发送看似由欺诈对象使用的合法金融机构发出的邮件。[523] 这些电子邮件在设计上使受害者难以辨别它们是伪造的电子邮件。[524] 电子邮件请求接收者透露和/或验证某些敏感信息。许多受害者上当受骗，透露了某些敏感信息，使违法者能够实施在线转账等犯罪行为。[525]

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

作案者总是企图篡改文件。如今，利用数字伪造，可以在不降低质量的前提下拷贝数字文件，并轻易地进行篡改。对取证专家而言，难以证明数据文件是否被篡改过，除非使用技术保护措施[526]来保护可能被篡改的文件。[527]

2.8.3 身份盗用

身份盗用这一术语既不会始终如一地定义，也不会始终如一地使用，它指的是利用欺诈手段获取和使用他人身份的犯罪行为。[528]实施这些犯罪行为可以无需借助技术方法[529]，也无需使用国际互联网技术。[530]

大规模的媒体报道、[531]分析身份盗用程度及其导致的损失的各种调查结果[532]以及近几年内发布的不计其数的法律和技术分析[533]容易使人们得出以下结论：与身份有关的犯罪行为是 21 世纪的特有现象。[534]但事实并非如此，因为与假冒身份以及伪造和滥用身份证明文件有关的犯罪行为已经存在超过一个世纪了。[535]早在 20 世纪 80 年代，新闻媒体就已深入报道了滥用与身份有关的信息的事件。[536]新出现的数字身份和信息技术的使用只是改变了违法者的方法和目标。[537]数字信息使用的日益增加为违法者获取与身份有关的信息提供了新的可能性。[538]因此，从工业化国家到信息社会的转型过程[539]对于身份盗用违法行为的发展具有重大影响。然而，尽管存在大量与国际互联网有关的身份盗用案件，数字化并未从根本上改变违法行为本身，而只是创造了新的目标，促进了新方法的开发。[540]对国际互联网技术日益增加的使用所造成的影响似乎被高估了。根据一项针对与身份有关的犯罪行为的方法分析得出的结果，身份盗用在很大程度上仍属于离线犯罪行为。[541] 2007 年，美国 20%的违法行为[542]属于在线骗局和数据泄露。[543]尽管近期事态发展有所变化，但离线身份盗用问题仍挥之不去。鉴于数字化的发展以及基于网络的服务的全球化已导致数字身份相关信息的使用日益增加，离线犯罪行为的持续重要性令人惊讶。[544]与身份有关的信息的重要性与日俱增，无论是在经济还是社会互动领域。过去，“良好的声誉”和良好的个人关系在商业经营以及日常交易中占据主导地位。[545]随着向电子商务转型，几乎不可能进行面对面的识别，因此对于参与社会和经济互动的人们来说，与身份有关的信息变得愈加重要。[546]这一过程可以描述为“工具化”，[547]即身份被转化为可量化的、与身份有关的信息。这一过程，以及“身份”一词更具哲学性的方面（定义[548]为个人特征的集合）与能够识别某一个人的、可量化的身份相关信息之间的区分，是极其重要的。转型过程不仅涉及身份盗用的互联网相关特点，因为发展的影响远超出计算机网络领域。如今，非面对面交易的要求，如信任和安全，[549]在总体经济而非只是电子商务企业中占据主导地位。其中一个示例是使用带有 PIN（个人识别码）的支付卡在超市内购买商品。

一般而言，被视为身份盗用的违法行为包含三个不同的阶段。[550]第一阶段，违法者获取与身份有关的信息。例如，这一步可以通过使用恶意软件或网络钓鱼攻击来实施。第二阶段的特点是在犯罪活动中在使用这些信息之前对与身份有关的信息进行交易。[551]一个例子是出售与身份有关的信息。[552]例如，信用卡记录的售价就曾高达 60 美元。[553]第三阶段是将与身份有关的信息用于犯罪行为。在大多数情况下，访问与身份有关的数据可使作案者能够实施进一步犯罪行为。[554]因此，作案者不会着眼于数据集本身，而着眼于将它们用于实施犯罪活动的能力。此类犯罪活动的例子可以是身份识别文件伪造或信用卡欺诈。[555]

在第一步中，用来获取数据的方法涵盖许多行为。违法者可以利用物理方法，如窃取带有与身份有关数据的计算机存储设备、搜索垃圾（“垃圾搜寻”[556]）或者邮件盗窃。[557]此外，他们可以使用搜索引擎来寻找与身份有关的数据。“谷歌黑客”或者“谷歌剁客”指的是使用复杂的搜索引擎查询来过滤大量的搜索结果，以便寻找与计算机安全问题有关的信息以及可以在身份盗用骗局中使用的个人信息。例如，作案者的其中一个目的是搜索不安全的密码保护系统，以便从中获取数据。[558]一些报告强调指出，搜索引擎的合法使用也会伴随用于非法目的的风险。[559]据报告，类似的问题也涉及文件共享系统。美国国会最近讨论了利用文件共享系统获取可被身份盗用者滥用的个人信息的可能性。[560]除此之外，违法者还可以利用内部人员获取信息，后者有权访问所储存的、与身份

有关的信息。美国计算机安全协会（CSI）于 2007 年开展的计算机犯罪与安全调查[561]表明，超过35%的回复者将其所在组织 20%以上的损失归咎于内部人员的泄密。2013 年的一项调查显示，23%的电子犯罪行为均与内部人士相关，53%的受访者认为，来自内部人士的攻击比外来者的攻击更具破坏性。[562]最后，作案者可以使用社会工程技术来说服受害者泄露其个人信息。最近几年，通过采用社会工程技术来操纵受害者，作案者设计了有效的骗局来获取秘密信息（如银行账号信息和信用卡数据）。[563]

作案者企图获取的数据类型也不是一成不变的。[564]他们最感兴趣的数据包括：社会保险号码和护照号码、出生日期、地址和电话号码以及密码。

社会保险号码（SSN）或者护照号码

例如，在美国，社会保险号码是一种典型的、与个人身份有关的数据例子，作案者常盯着这一目标。尽管社会保险号码的创建是为了保存一份准确的收入记录，但如今，它广泛用于证明某人的身份。[565]作案者可以使用社会保险号码以及获取的护照信息来开设银行账号、接管现有的银行账号、建立信誉或者迅速增加借款数额。[566]

出生日期、地址和电话号码

如果此类数据与其他信息（如社会保险号码）[567]相结合，那么它们一般只能用于实施身份盗用犯罪。访问到诸如生日和地址之类的额外信息，将有助于作案者绕过验证程序。与这种信息有关的最大危险之一是，它们目前在国际互联网上被广泛使用 — 或者是在各种各样与身份有关的论坛上自愿公开，[568] 或者是出于在网站上留下印记的法律要求。[569]

非银行账户密码

获取了这些账户的密码，作案者就可以改变账户的设置，使之为己所用。[570] 例如，他们可以接管一个电子邮件账户，并用其发送含有非法内容的邮件，或者接管用户在拍卖平台上使用的账号，并用该账号来销售赃物。[571]

银行账户的密码

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

身份盗用是一个严重问题，而且它的发案数量在与日俱增。[572] 2004 年上半年，3%的美国家庭感到自己成为了身份盗用的受害者。[573]2012 年，司法统计局宣布，在 2012 年，美国 16 岁以上人士中有 7%至少经历过一次身份盗用事件。[574]在英国，每年因身份盗用而给本国经济带来的损失高达 13 亿英镑。[575] 在澳大利亚，估计因身份盗用而带来的损失每年在不到 10 亿美元和超过 30 亿美元之间。[576] 2006 年，一次有关身份盗用的调查估计，美国在 2005 年因身份盗用而造成的损失高达 566 亿美元。[577]根据 2013 年身份盗用报告的估计， 2012 年的相关损失为 209 亿美元。损失不仅仅是经济上的，还包括对名誉的损害。[578] 在现实中，许多受害者并没有报告此类犯罪行为，同时金融机构也往往不希望大肆宣传客户的遭遇。身份盗用造成的真实损失可能远超出报告的损失。[579]

身份盗用基于以下事实，即国际互联网上几乎没有手段来验证用户的身份。在现实世界中识别人们的身份容易得多，而大多数形式的在线身份复杂得多。先进的身份识别工具（如使用生物测定信息）既昂贵，也尚未广泛应用。而针对在线行为的限制少之又少，因此使得身份盗用既容易，又有利可图。[580]

与“大数据”发展趋势密切相关的一个现象是：越来越多的身份信息正在“黑市”上待价而沽。若罪犯得以侵入拥有数百万客户记录的数据库，则大量此类数据便可能在日后被罪犯售出。例如，2014 年公布的一项研究表明，因数据泄露而在网络黑市上出售的身份信息规模涉及高达 3.6 亿个帐户产生的证书。[581]

2.8.4 设备滥用

只要使用一些基本的设备，就可以实施网络犯罪。[582] 诸如诽谤或在线欺诈等违法行为，除了一台计算机和国际互联网接入，再不需要别的设备，而且可以从某家公共的网吧来实施。更加老练和高级的违法行为则可能使用专业的软件工具来实施。

实施复杂违法行为所需的工具在国际互联网上唾手可得，[583]而且常常是免费的。更高级的工具则需花费数千美元。[584] 使用这些软件工具，违法者只需按下一个按钮，便可对其他的计算机系统发动攻击。如今，标准的攻击变得效率低下，原因是保护软件公司对当前可用的工具进行了分析，并对标准的黑客攻击已有所防范。引人注目的攻击通常是针对特定目标的。[585] 可用的软件工具[586]使违法者能够实施拒绝服务（DoS）工具[587]，设计计算机病毒，对加密的通信进行解密或者非法访问计算机系统。

目前，第二代软件工具可以自动执行许多网络骗局，并且能够使违法者在短时间内进行多次攻击。软件工具还可以简化攻击，使经验不足的计算机用户也能实施网络犯罪。垃圾邮件工具套件唾手可得，几乎使任何人都能发送垃圾电子邮件。[588] 如今，软件工具还可用来向文件系统上传文件或从中下载文件。由于专门设计的软件工具的可用性日益增大，潜在攻击者的数量已经急剧增多。不同国家以及国际社会正在采取一些立法措施来遏制网络骗局软件工具的增长势头，例如，通过对生产、销售或拥有这些工具的行为进行定罪。[589]

2.9 组合违法行为

参考书目（节选）： *Arquilla/Ronfeldt*, in The Future of Terror, Crime and Militancy, 2001; *Brandon,* Virtual Caliphate: Islamic extremists and the internet, 2008, available at: www.socialcohesion.co.uk/pdf/VirtualCaliphateExecutiveSummary.pdf; *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006; *Crilley*, Information warfare: New Battlefields – Terrorists, propaganda and the Internet, Aslib Proceedings, Vol. 53, No. 7 (2001); *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45, page 1033 *et seq.*; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf; *Gercke,* Cyberterrorism, How Terrorists Use the Internet, Computer und Recht, 2007, page 62 *et seq.*; *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.2, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Molander/Riddile/Wilson*, Strategic Information Warfare, 1996; *Rollins/Wilson*, Terrorist Capabilities for Cyberattack, 2007; *Schperberg*, Cybercrime: Incident Response and Digital Forensics, 2005; *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27; *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002; *Sieber/Brunst*, Cyberterrorism – the use of the Internet for terrorist purposes, Council of Europe Publication, 2007; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001; *Stenersen*, The Internet: A Virtual Training Camp?, in Terrorism and Political Violence, 2008; *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010; *Weimann*, How

Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003.

有许多术语可用于描述包含众多不同违法行为的复合骗局，包括网络恐怖主义、网络洗钱和网络钓鱼等。

2.9.1 网络恐怖主义

回溯到 20 世纪 90 年代，关于恐怖组织对网络使用的讨论着重于对关键基础设施发动基于网络的攻击，如交通和能源供应设施（“网络恐怖主义”）以及在武装冲突中使用信息技术（“网络战争”）。[590] 病毒和僵尸网络攻击的成功清楚地展现了网络安全中的薄弱环节。恐怖分子成功地进行基于国际互联网的攻击是可能的，[591] 但难以评估这种威胁的严重性。[592] 另外，相比当前的发展状况，当时的互联程度较低，这很有可能是此类事件很少见诸报端的主要原因之一，当然，有些国家出于利益考虑对成功的攻击保守秘密也是原因之一。因此，至少在过去，被风吹倒的树对电力供应造成的威胁，要比成功的黑客攻击造成的威胁大。[593]

但在 9·11 袭击之后，这种状况发生了改变。人们开始大量讨论恐怖分子使用信息通信技术进行破坏的问题。[594] 有报告指出，[595] 恐怖分子在准备攻击的过程中使用了国际互联网 [596]，更加推动了这种讨论。尽管这些攻击不是网络攻击，实施 9·11 袭击的恐怖分子并没有实施基于国际互联网的攻击，但国际互联网在攻击的准备阶段起到了重要作用。[597] 在这一背景中，恐怖组织使用国际互联网的各种不同方法开始浮出水面。[598] 如今，众所周知，恐怖分子利用信息通信技术和国际互联网来进行以下违法活动：

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

讨论焦点的这种转变，对与网络恐怖主义有关的研究产生了积极影响，原因是它突出了此前人们不知道的恐怖活动范围。但尽管综合治理方法相当重要，对关键基础设施发动基于国际互联网的攻击的威胁也应继续成为讨论的焦点。信息技术的弱点以及人们对它的日益依赖 [599]，使得我们必须将针对关键基础设施的、基于国际互联网的攻击纳入到防止和对抗网络恐怖主义的战略中来。

但是，尽管人们开展了密集的研究，与网络恐怖主义的斗争依然很艰难。对各国不同方法的比较表明，它们的战略中存在许多相似处。[600] 其中一个原因是国际社会认识到了为了应对国际恐怖主义的威胁，需要全球各国携手制定解决方案。[601] 但当前仍无法肯定这种方法是否成功，或者不同的法律体系以及不同的文化背景是否需要采用不同的解决方案。对这一问题的评估带来了一些独特的挑战，原因是除了对重大事件的报告，几乎没有多少可用的数据可用来进行科学分析。在确定恐怖组织使用信息技术时的威胁等级方面，也出现了同样的困难。这些信息大多数时候是保密的，因此只有情报部门才可以使用。[602] 甚至大家对“恐怖主义”这一术语的含义也没有达成一致。[603]例如，

提交美国国会的一份 CRS 报告声明，如果一个恐怖分子通过国际互联网订购了一张前往美国的机票，那么可以证明该恐怖分子在准备其攻击时使用了国际互联网。[604] 这看起来像是一个模糊的论点，原因是不能仅仅因为是恐怖分子订购了机票而将订购机票视为一种与恐怖分子有关的行为。

宣传活动

1998 年，在 30 个外国恐怖组织中，只有 12 个被美国国务院列入黑名单，这些组织在其网站上向公众宣传他们从事的活动。[605] 2004 年，美国和平研究所报告，几乎所有的恐怖组织都建立了网站，包括哈马斯、真主党、库尔德工人党和基地组织。[606] 恐怖分子还开始使用视频社区（如 YouTube ）来分发视频消息和进行宣传活动。[607] 网站和其他论坛的使用是颠覆破坏分子团体更加注重专业公关的标志。[608] 网站和其他媒体用于宣传活动，[609] 描述和公布恐怖组织活动的理由，[610] 并用于招募新成员 [611] 以及联络现有的成员和捐赠者。[612] 最近，网站还用于散发有关处决的视频。[613]

信息收集

国际互联网上可以接触到大量关于可能的目标的信息。[614] 例如，参与建造公共建筑的建筑师，通常会在其网站上发布建筑规划。如今，各种国际互联网服务都免费提供高分辨率的卫星照片，而在几年前，这些照片只能供世界上极少数的军事机构使用。[615] 此外，还可找到如何制造炸弹的指南，甚至一些虚拟训练营，它们以一种远程学习的方式来提供有关如何使用武器的指导。[616] 此外，从搜索机器人那里还可以获得一些没有采取足够保护措施的敏感信息或者机密信息，[617] 并可通过搜索引擎进行访问。2003 年，美国国防部被告知，一本与基地组织有关的训练手册中包含一些可以用于寻找潜在目标的详细信息的公共来源信息。[618] 2006 年，《纽约时报》报道说，某一政府网站上居然公布了如何制造核武器的基本信息，它们提供了关于伊拉克制造核武器方法的证据。[619] 澳大利亚媒体也报道了一则类似的事件：关于恐怖分子可能攻击的目标的详细信息被公布在一个政府网站上。[620] 2005 年，德国的新闻媒体报道说，调查人员在两名试图使用自制炸弹攻击公共交通系统的嫌疑人的计算机中，发现了从国际互联网上下载的、关于如何制造爆炸物的指南。[621]

准备在现实世界实施攻击

恐怖分子在准备攻击的过程中可以采用不同的方法来利用信息技术。发送电子邮件或者在论坛上留下消息就是一些例子，这将结合有关通信的内容来讨论。目前只讨论更为直接的在线准备方法。一些已发表的报告指出，恐怖分子目前在攻击的准备过程中使用了在线游戏。[622] 而国际互联网上存在着各种各样模拟现实世界的在线游戏。此类游戏的使用者可以利用游戏中的角色（化身），在虚拟世界中采取攻击行动。从理论上讲，这些在线游戏可以用来模拟攻击，但目前尚不确定，在线游戏究竟已在多大程度上牵涉到这种攻击行动中来。[623]

发布训练资料

国际互联网可用于散发培训资料，例如关于如何制造武器以及如何挑选攻击目标的指南。此类资料在网上大量存在。[624] 2008 年，西方的秘密特工发现了一个国际互联网服务器，它为培训资料的交换以及通信提供了基础。[625] 有报告指出，恐怖组织运营不同的网站来协调各种恐怖活动。[626]

通信

恐怖组织对信息技术的使用不限于运营网站和在数据库中开展研究。在 9·11 袭击之后开展的调查中报告，恐怖分子在协调其攻击时使用了电子邮件进行联络。[627] 新闻媒体曾就恐怖组织通过电子邮件互相交换关于目标和攻击者数量的详细指令进行过报道。[628] 通过使用加密技术和匿名通信方式，通信各方可以进一步增加执法机构识别和监控恐怖分子联络的难度。

恐怖分子筹集资金

大多数恐怖组织依赖从第三方获得的资金。追查这些金融交易已经成为 9·11 袭击之后与恐怖主义作斗争的一种重要手段。但这方面的主要困难之一在于以下事实，即发动攻击所需的资金并不一定很多。[629] 在恐怖分子筹集资金时，可以采用几种方式来使用国际互联网服务。恐怖组织可以利用电子支付系统来接受在线捐赠。[630] 他们可以使用网络来公布关于如何捐赠的信息，例如，应当使用哪个银行账号来捐赠。这方面的一个例子是“解放党”组织曾经为可能的捐赠者公布过银行账号信息。[631] 另一种方法是进行在线信用卡捐赠。爱尔兰共和军（IRA）就是最先通过信用卡提供捐赠的恐怖组织之一。[632] 对恐怖组织而言，这两种方法都存在一定的风险，即公布的信息会被执法机构发现，并用来追查这些金融交易。因此，这有可能使匿名的电子支付系统变得更加流行。为了不被发现，恐怖组织试图通过一些非可疑的团体，如慈善组织，来掩盖其筹资活动。另一种（与国际互联网有关的）方法是经营虚假的互联网商店。在国际互联网上创建一个在线商店相对比较简单。网络的最大优势之一是业务可以在全世界范围内进行。要证明在这些网站上进行的金融交易不是普通买卖而是为恐怖组织提供的捐赠，是非常困难的。这可能需要对每一笔交易进行调查，但如果在线商店是在不同的管辖地经营的，或者使用了匿名的支付系统，那么这样做的难度将非常大。[633]

对关键基础设施实施攻击

除了欺诈和身份盗用等普通的网络犯罪之外，针对关键基础设施的进攻可能成为恐怖分子的新目标。对信息技术的依赖愈来愈高，使关键基础设施变得更易遭到攻击。[634] 针对用计算机和通信网络连接在一起的互连系统而进行的攻击更是这样。[635] 在这些情形中，因对网络实施攻击而造成网络中断，其损失远超单个系统的失效。即使是短时间的服务中断，也可能对电子商务企业造成巨大的经济损失，而且不仅仅对民用设施是这样，对军用基础设施和服务也一样。[636] 调查或者甚至防止这些攻击的发生，是一项独特的挑战。[637]与物理攻击不同，攻击者不需要出现在攻击现场，[638] 并且在实施攻击的同时，攻击者可以使用匿名通信手段和加密技术来隐藏其身份。[639]正如以上所强调的那样，对此类攻击的调查需要采用特殊的程序手段、调查技术以及训练有素的调查人员。[640]

关键基础设施被广泛认为是恐怖分子攻击的一大潜在目标，原因是它对一个国家的可持续发展和稳定无疑是至关重要的。[641] 如果某种基础设施丧失作用或遭到破坏，将对国家的国防或经济安全产生重大影响，那么这种基础设施将被认为是一种关键基础设施。[642] 以下这些尤其重要：电力系统、电信系统、天然气和石油储运系统、银行和金融系统、交通系统、供水系统和应急服务系统。“卡特里娜”飓风对美国服务的破坏而导致的内乱程度，突显了社会对这些系统可用性的依赖程度。[643] 恶意软件“超级工厂病毒（Stuxnet）”强调了以关键基础设施为重点攻击对象的、基于互联网的攻击所造成的新兴威胁。[644] 2010 年，白俄罗斯的一家 安全公司发现了一种新的恶意软件。[645] 对于该软件导致的操作、设计者以及动机的研究仍在继续，目前为止尚未查明全部事实，尤其是设计者的归属和动机。[646] 然而，特别在软件的功能运行方面，目前似乎已掌握了相当充分的事实依据：

据报道，这一具有 4000 多个功能的复杂软件[647] 主要针对工业控制系统（ICS）[648] – 尤其是技术公司西门子生产的同类系统。[649]该病毒通过可移除驱动器传播，使用四个零日攻击感染计算机系统。[650] 报道称，受感染的计算机系统主要来自伊朗、印度尼西亚和巴基斯坦，但也有部分来自美国和欧洲国家。[651] 虽然该恶意软件经常被定性为高度复杂的软件，但也有报道质疑其精密程度。[652]

如上所述，设计者归属和动机的确定更加困难，目前仍存在高度不确定性。新闻报道和研究推测，该软件的目标可能是伊朗的铀浓缩设施，并导致该国的核计化延迟。[653]

从该恶意软件的发现可以得出两个主要结论。首先，该事件突显了关键基础设施在很大程度上依赖于计算机技术，并且攻击是可能发生的。其次，该软件是通过可移除驱动器等其他方法传播的这一事实，强调了简单地中断计算机系统和国际互联网的连接并不能阻止攻击。

关键基础设施对于信息通信技术的依赖远不止在能源和核工业领域。这一点可以通过强调一些与航空运输有关的事件加以证明，航空运输在大多数国家内也被视为关键基础设施的一部分。其中一个潜在的攻击目标是登机系统。世界大多数机场的登机系统都已使用互连的计算机系统。[654] 2004 年，Sasser 计算机蠕虫病毒 [655] 感染了全世界数百万台计算机，其中就包括一些大型航空公司的计算机系统,导致一些航班被迫取消。[656]

另一个潜在目标是网上订票系统。如今，很大一部分机票是网上订购的。航空公司使用信息技术来进行各种操作。所有的大型航空公司都允许其顾客在线购买机票。与其他电子商务活动一样，这些在线业务可能成为攻击者的目标。用来攻击基于互联网的服务的一种常见方法是拒绝服务攻击（DoS）。[657] 2000 年，在短时间内，美国有线新闻网（CNN）、易趣（eBay）和亚马逊（Amazon）等一些知名公司就遭到了拒绝服务攻击。[658] 结果是，一些服务在数小时甚至几天内无法使用。[659] 航空公司同样也受到过拒绝服务攻击的影响。2001 年，德国汉莎航空公司就成为了一次攻击的目标。[660]

最后，对针对关键航空运输基础设施的、与国际互联网有关的攻击而言，另一个潜在的目标是机场控制系统。计算机控制的飞行控制系统的脆弱性，在 1997 年针对美国 Worcester 机场的黑客攻击中暴露无遗。[661] 在此次黑客攻击中，攻击者使机场塔台的电话服务陷入瘫痪，并关闭了用于管理跑道灯光的控制系统。[662]

2.9.2 网络战争

2007 年在爱沙尼亚和 2008 年在格鲁吉亚境内发生针对计算机系统的攻击以及发现了“超级工厂计算机病毒（Stuxnet）”[663] 之后，“网络战争”一词频繁用于描述以下详细介绍的情况 – 尽管对于这一术语的使用仍存在疑问。

术语和定义

关于网络战争，目前尚无统一的术语或广为接受的定义。使用的其他术语包括信息战争、电子战争、网络战（cyberwar/netwar）和信息行动。[664] 这些术语通常用于描述在利用国际互联网发动的战争中对于信息通信技术的使用。更加严格的定义将此类活动定义为，侧重于信息的全部形式和程度的管理和利用的武装冲突方法，目的在于实现决定性的军事优势，尤其是在联合和合并的环境中。[665] 其他更为广义的定义包含任何形式的电子冲突，其中信息属于值得征服或破坏的战略资产。[666]

辩论的发展

数十年来，该议题一直属于争议性问题。[667] 人们的关注点最初集中于以计算机作为媒介的攻击或基于计算机的攻击对于传统战争的取代。[668] 在此方面，不参与战斗即可战胜任何敌人的能力从一开始就是辩论核心的关键部分之一。[669] 另外，基于网络的攻击的成本通常低于传统军事行动，[670] 甚至小国也可以发动此类攻击。尽管经常引用一些具体案例，[671] 但辩论的主要方面仍具有非常高的假设性。其中最常引用的两个例子是针对爱沙尼亚和格鲁吉亚的计算机攻击。然而，将某一攻击归类为战争行为需要满足特定的标准。

2007 年，爱沙尼亚经历了关于撤除第二次世界大战纪念碑的激烈辩论，首都甚至出现了街头骚乱。[672] 除传统的抗议形式外，爱沙尼亚当时还发现了多起针对政府和私营企业网站以及在线服务的

计算机相关攻击事件，[673]形式包括网站篡改[674]、针对域名服务器的攻击和分布式拒绝服务攻击（DDoS），其中使用了僵尸网络。[675] 关于后者，专家后来解释称，针对爱沙尼亚政府机构官方网站的攻击[676]之所以成功，只因保护措施不足。[677] 这些攻击的影响以及它们的起源随后成为一些争议性讨论的主题。尽管新闻报道[678]和文章[679] 指出这些攻击差点关闭了该国的数字基础设施，但更为可靠的研究表明，这些攻击的影响在受影响的计算机系统和服务停用的持续时间方面都非常有限。[680] 在确定攻击起源方面也发生了类似的辩论。虽然在攻击期间有报告称俄罗斯联邦领土是攻击起源[681]，但攻击分析显示它们实际上涉及 170 多个国家。[682] 即使具有政治动机的攻击也不一定构成战争行为。因此，需要将爱沙尼亚案例从列表中排除。尽管这些攻击是针对政府和私营企业以及在线服务[683]的、与计算机有关的攻击，并且形式包括网站篡改[684] 和分布式拒绝服务攻击（DDoS）[685]，但是这类攻击不能被定性为网络战争，因为它们既未构成武力行为，也不是在两个主权国家爆发冲突期间发生的。

在上述两个攻击案例中，2008 年针对格鲁吉亚计算机系统的攻击最接近与战争有关的攻击。在俄罗斯联邦与格鲁吉亚之间传统的武装冲突 [686] 背景下，发现了多起针对格鲁吉亚政府和企业网站[687] （包括网站篡改和分布式拒绝服务攻击）的、与计算机有关的攻击事件。[688] 如同爱沙尼亚事件一样，针对格鲁吉亚的攻击起源也在事后成为辩论的焦点。尽管一些新闻报道 [689] 似乎查明了攻击的地理起源，但侧重于技术的研究指出，僵尸网络的使用使得确定攻击起源的工作更加困难。[690] 由于无法确定攻击起源，以及所发现的行为与传统战争存在巨大差异，因此很难将这些它们定性为网络战争。

鉴于有关这一现象的辩论非常重要，应当指出，这类攻击并非前所未有的现象。通过国际互联网传播宣传内容，以及针对军事同盟的计算机系统的攻击是一个颇为普遍的概念。早在南斯拉夫战争期间，就已经发现来自塞尔维亚的针对北大西洋公约组织（NATO）计算机系统的攻击。[691] 作为回应，报告称北约成员国也参与了针对塞尔维亚计算机系统的类似攻击。[692] 旨在破坏对手作战决心的进一步计算机宣传以及其他形式的心理战（PSYOPS）已经得到高度利用。[693]

区分的重要性

潜在的战争有关行为与其它形式的信息通信技术滥用（例如网络犯罪和恐怖主义对国际互联网的使用）存在许多相似性。因此，“网络犯罪”、“恐怖主义对国际互联网的使用”以及“网络战争”等术语经常互换使用。但由于适用的法律框架差别很大，因此进行区分是非常重要的。尽管一般通过定罪方式处理网络犯罪行为，但与网络战争有关的规则和程序在很大程度上则受国际法的管制，尤其是《联合国宪章》。

2.9.3 网络洗钱

2013 年，电子货币提供商“Liberty Reserve”的关闭成为头条新闻[694]，而估值高达 60 亿美元的涉案金额亦令其成为史上最大的网络洗钱案件。[695]2013 年，美国财政部公布了与此案件相关的详细调查结果。[696]国际互联网正促使洗钱犯罪的方式发生转变。尽管数量更大的、传统的洗钱技术仍有诸多优势，但国际互联网也提供了若干优势。在线金融服务可以使人们非常迅速地完成多项涉及全世界的金融交易。国际互联网有助于克服对实体金融交易的依赖。随着在遏制对实体货币的依赖方面迈出第一步，电子转账取代了传统的现金转移，但是，各国政府采取了更加严格的规定来侦查可疑的电子转账，迫使违法者转而研究一些新的技术。在与洗钱犯罪活动作斗争的过程中，对可疑交易的侦查是基于金融机构在转账方面的义务来进行的。[697]

洗钱通常分为三步：布置、分层以及综合。

关于大量现金的处置，使用国际互联网或许不具备许多实际的优势。[698] 不过，对违法者而言，在分层（或者说掩饰）阶段，国际互联网特别有用。在这种背景下，当洗钱者利用在线赌场进行分层时，要调查网络洗钱就变得特别困难了。[699]

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

虚拟货币的使用

推动虚拟货币发展的一个关键因素是小额支付（例如，为了支付网上下载一篇文章不到 10 美分的费用），这种时候，使用信用卡就成了问题。随着小额支付的需求日益增大，包括“虚拟金币”在内的虚拟货币应运而生。虚拟金币是以账号为基础的支付系统，金币的价格靠黄金储备来支持。用户可以在线开设电子金币账号，通常无需注册。有些提供商甚至能够进行直接的点对点（个人对个人）转账或者现金提款。[700] 违法者可以在不同的国家开设电子金币账号，并且将它们结合起来，使为了洗钱和资助恐怖活动而使用金融工具变得更加复杂化。账号持有者还可以在注册期间使用不准确的信息来掩盖其身份。[701]

除简单的虚拟货币外，还存在一些将虚拟方面与匿名性相结合的货币，例如比特币（*Bitcoin*），一种使用点对点技术的虚拟货币。[702] 尽管这是一种分散式系统，不需要中心中介机构来确保交易的合法性，但 2011 年内的成功攻击突显了与这类分散式虚拟货币有关的漏洞/风险。[703] 如果犯罪分子使用此类匿名货币，则会限制执法机构通过追踪资金转账确定嫌疑人的能力[704] – 例如，在与商业性儿童色情制品有关的案件中。[705]

在线赌场的使用

与开设实体赌场不同，开设在线赌场无需大笔的金融投资。[706] 此外，各国对在线和离线赌场的管制通常各不相同。[707] 只有当赌场留有详细记录，并将它们提供给执法机构时，才有可能跟踪资金转移情况，证明所转资金并非赢来的钱，而是洗钱的结果。

当前对基于国际互联网的金融服务的法律管制，不如对传统金融服务的管制那样严格。除了这种法律上的差异之外，管制的困难还来自难以进行客户验证 – 如果金融服务提供商和客户从不见面，那么准确的验证可能只是流于形式。[708] 另外，缺乏个人合同使得难以应用传统的“认识你的客户”程序。国际互联网转账常常涉及许多国家中提供商的跨国参与。最后，当提供商允许客户以点对点模式转移资金时，监控交易的工作变得异常困难。

2.9.4 网络钓鱼

违法者已经开发了一些技术来从用户手中获取个人信息，包括间谍软件[709] 和“网络钓鱼”攻击。[710] “网络钓鱼”指的是想方设法使受害者泄露个人/秘密信息的违法行为。[711]有各种不同类型的“网络钓鱼”攻击，[712]但基于电子邮件的网络钓鱼攻击包含三个主要阶段。在第一个阶段中，违法者确定提供在线服务的合法公司，并与它们瞄上的客户进行电子通信，如金融机构。违法者设计一些类似于合法网站的网站（“钓鱼网站”），要求受害者执行通常的登录程序，这样，违法者就可以获得受害者的个人信息（如账号和在线银行密码）。

为了使用户能够进入这些经过伪装的欺骗网站，违法者向他们发送类似于合法公司发出的电子邮件，[713] 这往往还导致商标侵权。[714] 这种冒充合法公司发出的电子邮件要求接收者登录，以便更新或者进行安全检测，或者，假如用户不肯合作，违法者就采用威胁手段（如威胁关闭用户的账号）。这种冒充的电子邮件往往包含一个链接，将使受害者点击后进入欺骗网站，以避免用户手动

输入合法金融机构的正确网址。违法者还研发了一些先进的技术来防止用户意识到他们进入的不是真正的金融机构网站。[715]

一旦个人信息被泄露，违法者就会登录受害者的账号，并实施各种犯罪，如转移资金、申请护照或新账号等。“网络钓鱼”成功攻击的数量在增多，证明了它的破坏潜力。[716] 2007 年 4 月，向反网络钓鱼工作组（APWG）[717] 报告的、特别的“网络钓鱼”网站超过了 55 000 家。[718] 2014 年 1 月，检测到的专门从事“网络钓鱼”网站的数量升至近 43 000 家。[719] “网络钓鱼”技术不仅限于获取在线银行业务的密码。违法者还试图获取进入计算机的密码、拍卖平台和社会保险号码，这些在美国都是特别重要的信息，可以导致“身份盗用”违法行为的发生。[720]

87 Other terminology used includes information technology crime and high-tech crime. See, in this context: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, International Journal of Law and Information Technology, 2002, Vol. 10, No. 2, page 144.

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

89 *Nhan/Bachmann* in Maguire/Okada (eds), Critical Issues in Crime and Justice, 2011, page 166.

90 Regarding this relationship, see also: *Sieber* in Organised Crime in Europe: The Threat of Cybercrime, Situation Report 2004, page 86.

91 Crimes related to computer networks, Background paper for the workshop on crimes related to the computer network, 10th UN Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.187/10, page 5; available at: www.uncjin.org/Documents/congr10/10e.pdf.

92 With regard to the definition, see also: *Kumar*, Cyber Law, A view to social security, 2009, page 29.

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

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

95 *Arti*cle 1, Definitions and Use of Terms,

For the purposes of this Convention:

1. “cyber crime” means conduct, with respect to cyber systems, that is classified as an offense punishable by this Convention;

[...]

96 See: *Hayden*, Cybercrime’s impact on Information security, Cybercrime and Security, IA-3, page 3.

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

98 Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq.*

99 Universal serial bus (USB)

100 Article 4 – Data Interference:

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

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

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

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

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

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

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

[107] Art. 2 (Illegal access), Art. 3 (Illegal interception), Art. 4 (Data interference), Art. 5 (System interference), Art. 6 (Misuse of devices). For more information about the offences, see below: § 6.2.

[108] Art. 7 (Computer-related forgery), Art. 8 (Computer-related fraud). For more information about the offences, see below: § 6.2.

[109] Art. 9 (Offences related to child pornography). For more information about the offences, see below: § 6.2.

[110] Art. 10 (Offences related to infringements of copyright and related rights). For more information about the offences, see below: § 6.2.

[111] See below: § 2.5.

[112] See below: § 2.6.

[113] See below: § 2.7.

[114] See below: § 2.8.

[115] See below: § 2.9.1

[116] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq.*

[117] Regarding the related challenges, see: *Slivka/Darrow*; Methods and Problems in Computer Security, Journal of Computers and Law, 1975, page 217 *et seq.*

[118] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

[119] See: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

[120] *Ruggles/Miller/Kuh/Lebergott/Orcutt/Pechman*, Report of the Committee on the Preservation and Use of Economic Data, 1965, available at: www.archive.org/details/ReportOfTheCommitteeOnThePreservationAndUseOfEconomicData1965.

[121] *Miller*, The Assault on Privacy-Computers, 1971.

[122] *Westin/Baker*, Data Banks in a Free Society, 1972.

[123] For an overview about the debate in the US and Europe, see: *Sieber*, Computer Crime and Criminal Law, 1977.

[124] *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 48.

[125] *Stevens*, Identifying and Charging Computer Crimes in the Military, Military Law Review, Vol. 110, 1985, page 59.

[126] *Gemignani*, Computer Crime: The Law in '80, Indiana Law Review, Vol. 13, 1980, page 681.

[127] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*

[128] For an overview about cases see: *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 5, available at: www.mekabay.com/overviews/history.pdf.

[129] *Freed*, Materials and cases on computer and law, 1971, page 65.

[130] *Bequai*, The Electronic Criminals – How and why computer crime pays, Barrister, Vol. 4, 1977, page 8 *et seq.*

[131] Criminological Aspects of Economic Crimes, 12th Conference of Directors of Criminological Research Institutes, Council of Europe, Strasbourg, 1976, page 225 *et seq.*; Staff Study of Computer Security in Federal Programs; Committee on Governmental Operations, the 95th Congress 1 Session, United States Senate, February 1977.

[132] *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Bequai*, Computer Crime: A Growing and Serious Problem, Police Law Quarterly, Vol. 6, 1977, page 22.

133 *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 527.

134 Regarding the number of the cases in early cybercrime investigations, see: *Schjolberg*, Computers and Penal Legislation, A study of the legal politics and a new technology, 1983, page 6, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

135 *Quinn*, Computer Crime: A Growing Corporate Dilemma, The Maryland Law Forum, Vol. 8, 1978, page 58, Notes – A Suggested Legislative Approach to the Problem of Computer Crime, Washington and Lee Law Review, 1981, page 1173.

136 *Nycum*, The criminal law aspects of computer abuse: Applicability of federal criminal code to computer abuse, 1976

137 Federal Computer Systems Protection Act of 1977. For more information, see: *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 2, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf; *McLaughlin*, Computer Crime: The Ribicoff Amendment to United States Code, Title 18, Criminal Justice Journal, 1978, Vol. 2, page 217 *et seq.*; *Nycum*, Legal Problems of Computer Abuse, Washington University Law Quarterly, 1977, page 531.

138 Third Interpol Symposium on International Fraud, France 1979.

139 Computer Abuse: The Emerging Crime and the Need for Legislation, Fordham Urban Law Journal, 1983, page 73.

140 *BloomBecker*, The Trial of Computer Crime, Jurimetrics Journal, Vol. 21, 1981, page 428; *Schmidt*, Legal Proprietary Interests in Computer Programs: The American Experience, Jurimetrics Journal, Vol. 21, 1981, 345 *et seq.*; *Denning*, Some Aspects of Theft of Computer Software, Auckland University Law Review, Vol. 4, 1980, 273 *et seq.*; *Weiss*, Pirates and Prizes: The Difficulties of Protecting Computer Software, Western State University Law Review, Vol. 11, 1983, page 1 *et seq.*; *Bigelow*, The Challenge of Computer Law, Western England Law Review, Vol. 7, 1985, page 401; *Thackeray*, Computer-Related Crimes, Jurimetrics Journal, 1984, page 300 *et seq.*

141 *Andrews*, The Legal Challenge Posed by the new Technology, Jurismetrics Journal, 1983, page 43 *et seq.*

142 *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

143 *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

144 *Schjolberg*, Computer-related Offences, Council of Europe, 2004, page 4, available at: www.cybercrimelaw.net/documents/Strasbourg.pdf.

145 Computer-related criminality: Analysis of Legal Politics in the OECD Area, 1986

146 Computer-related crime: Recommendation No. R. (89) 9.

147 Regarding the transnational dimension of cybercrime see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7.

148 Regarding the impact of the speed of data exchange on cybercrime investigation, see: § 3.2.10.

149 Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17; Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

150 A/RES/45/121 adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm

151 UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at: www.uncjin.org/Documents/EighthCongress.html.

152 The term “phishing” describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to “phish” for passwords and financial data from a sea of Internet users. The use of “ph” linked to popular hacker naming conventions. For more information, see: § 2.9.4.

153 Botnets is a short term for a group of compromised computers running a software that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4.

154 *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006.

155 *Velasco San Martin,* Jurisdictional Aspects of Cloud Computing, 2009; *Gercke*, Impact of Cloud Computing on Cybercrime Investigation, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq*

156 See for example: Big Data for Development: Challenges & Opportunities, UN Global Pulse, 2012; Sircar, Big Data: Countering Tomorrow's Challenges, Infosys Labs Briefings, Vol. 11, No. 1, 2013;

157 Hartmann/Steup, The Vulnerability of UAVs to Cyber Attacks – An Approach to the Risk Assessment, published in Podins/Stinissen/Maybaum, 5th International Conference on Cyber Conflicts, 2013; Kim/Wampler/Goppert/Hwang/Aldridge, Cyber attack vulnerabilities analysis for unanned areal vehicles, American Institute of Aeronautics and Astronautics, 2012.

158 *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 308, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

159 *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

160 Regarding the emerging importance of crime statistics, see: *Osborne/Wernicke*, Introduction to Crime Analysis, 2003, page 1 *et seq.*, available at: www.crim.umontreal.ca/cours/cri3013/osborne.pdf.

161 2009 Internet Crime Report, Internet Crime Complaint Center, 2009, available at: www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

162 German Crime Statistics 2009, available at www.bka.de. As this number also includes traditional crimes that involved Internet technology at any stage of the offence, the increase of cases cannot necessarily be used to determine the specific development in the typology-based crime fields.

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

164 Regarding challenges related to crime statistics in general, see: *Maguire* in Maguire/Morgan/Reiner, The Oxford Handbook of Criminology, 2007, page 241 *et seq.* available at: www.oup.com/uk/orc/bin/9780199205431/maguire_chap10.pdf.

165 See in this context: Overcoming barriers to trust in crimes statistics, UK Statistics Authority, 2009, page 9, available at: www.statisticsauthority.gov.uk/.../overcoming-barriers-to-trust-in-crime-statistics--england-and-wales---interim-report.pdf.

166 *Alvazzi del Frate*, Crime and criminal justice statistics challenges in Harrendorf/Heiskanen/Malby, International Statistics on Crime and Justice, 2010, page 168, available at: www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

167 Computer Crime, Parliamentary Office of Science and Technology, Postnote No. 271, Oct. 2006, page 3.

168 Regarding the related challenges, see: *Kabay*, Understanding Studies and Surveys of Computer Crime, 2009, available at: www.mekabay.com/methodology/crime_stats_methods.pdf.

169 The US Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform the authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack," explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, – available at: www.heise-security.co.uk/news/80152. See also: Comments on Computer Crime – Senate Bill S. 240, Memphis State University Law Review, 1980, page 660.

170 See *Mitchison/Urry*, Crime and Abuse in e-Business, IPTS Report, available at: www.jrc.es/home/report/english/articles/vol57/ICT2E576.htm; *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol. 2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf.

171 See *Collier/Spaul*, Problems in Policing Computer Crime, Policing and Society, 1992, Vol.2, page, 310, available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.66.1620&rep=rep1&type=pdf; *Smith*, Investigating Cybercrime: Barriers and Solutions, 2003, page 2, available at: www.aic.gov.au/conferences/other/smith_russell/2003-09-cybercrime.pdf.

172 In fact, newspapers as well as TV stations limit their coverage of successful Internet investigations to spectacular cases such as the identification of a paedophile by descrambling manipulated pictures of the suspect. For more information about the case and the coverage, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp.

[173] See SOCA, International crackdown on mass marketing fraud revealed, 2007, available at: www.soca.gov.uk/downloads/massMarketingFraud.pdf.

[174] In the 2006 NW3C Internet Crime report, only 1.7 per cent of the reported total USD losses were related to the Nigerian Letter Fraud, but those cases that were reported had an average loss of USD 5 100 each. The number of reported offences is very low, while the average loss of those offences is the high.

[175] With regard to this conclusion, see also: Cybercrime, Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO Document GAO-07-705, page 22. *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[176] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 1.29.

[177] See in this context: *Hyde-Bales/Morris/Charlton*, The police recording of computer crime, UK Home Office Development and Practice Report, 2004.

[178] Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport, page 15.

[179] National Fraud Information Center, 2007 Internet Fraud Statistics, 2008, available at: www.fraud.org/internet/intstat.htm.

[180] See Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report.

[181] 2nd ISSA/UCD Irish Cybercrime Survey, 2008, available at: www.issaireland.org/2nd%20ISSA%20UCD%20Irish%20Cybercrime%20Survey%20-%20Results%2017DEC08.pdf.

[182] Symantec Intelligence Quarterly, April-June 2010, available at www.symantec.com/business/theme.jsp?themeid=threatreport.

[183] 2010 CSO CyberSecurity Watch Survey, 2010.

[184] 2008 CSI Computer Crime and Security Survey, 2009, page 15.

[185] Symantec Global Internet Security Threat Report, Trends for 2009, 2010, available at: www.symantec.com/business/theme.jsp?themeid=threatreport, page 7,

[186] Net Losses, Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014, page 2.

[187] Net Losses, Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014, page 8.

[188] Net Losses, Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, CSIS, 2014, page 8.

[189] 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2013.

[190] Goodin, PlayStation Network breach will cost Sony $ 171m, The Register, 24.05.2011, available at: www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/.

[191] See 2005 FBI Computer Crime Survey, page 10.

[192] See: § 2.4.

[193] *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62; ECPAT, Violence against Children in Cyberspace, 2005, page 54; Council of Europe Organized Crime Situation Report 2005, Focus on Cybercrime, page 41.

[194] *Bialik*, Measuring the Child-Porn Trade, The Wall Street Journal, 18.04.2006.

[195] Computer Security Institute (CSI), United States.

[196] The CSI Computer Crime and Security Survey 2007 is available at: www.gocsi.com/

[197] See CSI Computer Crime and Security Survey 2007, page 1, available at: www.gocsi.com/. Having regard to the composition of the respondents, the survey is likely to be relevant for the United States only.

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

199 See below: § 2.4.

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

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

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

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

204 See *Levy*, Hackers, 1984; Hacking Offences, Australian Institute of Criminology, 2005, available at: www.aic.gov.au/publications/htcb/htcb005.pdf; *Taylor*, Hacktivism: In Search of lost ethics? in *Wall*, Crime and the Internet, 2001, page 61; *Yee*, Juvenile Computer Crime – Hacking: Criminal and Civil Liability, Comm/Ent Law Journal, Vol. 7, 1984, page 336 *et seq.*; Who is Calling your Computer Next? Hacker!, Criminal Justice Journal, Vol. 8, 1985, page 89 *et seq.*; The Challenge of Computer-Crime Legislation: How Should New York Respond?, Buffalo Law Review Vol. 33, 1984, page 777 *et seq.*

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

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

207 *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

208 *Musgrove*, Net Attack Aimed at Banking Data, Washington Post, 30.06.2004.

209 *Sieber*, Council of Europe Organised Crime Report 2004, page 66.

210 *Sieber*, Council of Europe Organised Crime Report 2004, page 65. Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

211 Hacking into a computer system and modifying information on the first page to prove the ability of the offender can – depending on the legislation in place – be prosecuted as illegal access and data interference. For more information, see below: § 6.2.1 and § 6.2.4.

212 The term "hacktivism" combines the words hack and activism. It describes hacking activities performed to promote a political ideology. For more information, see: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf. Regarding cases of political attacks, see: *Vatis*, cyberattacks during the war on terrorism: a predictive analysis, available at: www.ists.dartmouth.edu/analysis/cyber_a1.pdf.

213 A hacker left messages on the website that accused the United States and Israel of killing children. For more information, see BBC News, "UN's website breached by hackers", available at: http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/6943385.stm

214 The abuse of hacked computer systems often causes difficulties for law-enforcement agencies, as electronic traces do not often lead directly to the offender, but first of all to the abused computer systems.

215 Regarding different motivations and possible follow-up acts, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1;

[216] The Online-Community HackerWatch publishes reports about hacking attacks. Based on their sources, more than 250 million incidents were reported in the month of August 2007. Source: www.hackerwatch.org.

[217] Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5.

[218] See Heise News, Online-Computer werden alle 39 Sekunden angegriffen, 13.02.2007, available at: www.heise.de/newsticker/meldung/85229. The report is based on an analysis from Professor Cukier.

[219] For an overview of examples of successful hacking attacks, see http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

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

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

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

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

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

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

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

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

[228] Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see: *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. For more information about botnets see below: § 3.2.9.

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

[230] See in this context Art. 2, sentence 2, Convention on Cybercrime.

[231] *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.264.

[232] One example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a) until 2007, when the provision was changed. The following text is taken from the old version of Section 202a – Data Espionage:

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

233 With regard to targeted attacks see for example: *Sood/Enbody*, Targeted Cyber Attacks: Multi-staged Attacks Driven by Exploits and Malware, 2010. With regard to trends towards targeted attack see: Blurring Boundaries, Trend Micro Security Predictions for 2014 and Beyond, Trend Micro, 2014.

234 Targeted Cyber Attacks, GFI White Paper, 2009, page 5.

235 With regard to details related to the damage of targeted attacks see: *Kaspersky*, IT Security Risks Survey 2014.

236 For the modus operandi, see *Sieber*, Council of Europe Organised Crime Report 2004, page 102 *et seq.*; *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

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

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

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

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

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

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

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

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

245 See the information offered by an anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See: *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

246 Regarding the elements of an Anti-Cybercrime Strategy, see below: § 4.

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

248 Physical research proves that it can take a very long time to break encryption, if proper technology is used. See *Schneier*, Applied Cryptography, page 185. For more information regarding the challenge of investigating cybercrime cases that involve encryption technology, see below: § 3.2.14.

249 The Council of Europe Convention on Cybercrime contains no provision criminalizing data espionage.

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

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

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

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

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

255 See *Hackworth*, Sypware, Cybercrime & Security, IIA-4, page 5.

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

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

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

259 Regular hardware checks are a vital part of any computer security strategy.

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

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

262 For more information on the phenomenon of phishing, see below: § 2.9.4.

263 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2013.

264 2013 Cost of Data Breach Study: Global Analysis, Ponemon Institute, 2013.

265 Goodin, PlayStation Network breach will cost Sony $ 171m, The Register, 24.05.2011, available at: www.theregister.co.uk/2011/05/24/sony_playstation_breach_costs/.

266 *Finkle*, 360 million newly stolen credentials on black market: cybersecurity firm, Reuters, 25.02.2014.

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

268 With the fall in price of server storage space, the external storage of information has become more popular. Another advantage of external storage is that information can be accessed from every Internet connection.

269 Regarding the interception of VoIP to assist law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf. Regarding the potential of VoIP and regulatory issues, see: *Braverman*, VoIP: The Future of Telephony is now…if regulation doesn't get in the way, The Indian Journal of Law and Technology, Vol.1, 2005, page 47 *et seq.*, available at: www.nls.ac.in/students/IJLT/resources/1_Indian_JL&Tech_47.pdf.

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

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

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

273 With regard to the time necessary for decryption, see below: § 3.2.14.

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

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

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

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

278 e.g. the electromagnetic emission caused by transmitting the information displayed on the screen from the computer to the screen.

279 For more details on legal solutions, see below: § 6.2.4.

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

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

282 A computer virus is software that is able to replicate itself and infect a computer, without the permission of the user, to harm the computer system. See *Spafford*, The Internet Worm Program: An Analysis, page 3; *Cohen*, Computer Viruses – Theory and Experiments, available at: http://all.net/books/virus/index.html; *Adleman*, An Abstract Theory of Computer Viruses, Advances in Cryptography – Crypto, Lecture Notes in Computer Science, 1988, page 354 *et seq.* Regarding the economic impact of computer viruses, see: *Cashell/Jackson/Jickling/Webel*, The Economic Impact of Cyber-Attacks, page 12; Symantec Internet Security Threat Report,Trends for July-December 2006, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

283 *Kabay*, A Brief History of Computer Crime: An Introduction for Students, 2008, page 23, available at: www.mekabay.com/overviews/history.pdf.

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

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

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

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

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

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

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

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

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

293 Annual Report, Pandalabs, 2013.

294 Kaspersky Press Release, 10.12.2013, available at: www.kaspersky.com/about/news/virus/2013/number-of-the-year.

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

Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf..

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

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

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

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

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

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

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

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

304 July, 2009 South Korea and US DDosc Attacks, Arbor Networks, 2009, available at: www.idcun.com/uploads/pdf/July_KR_US_DDoS_Attacks.pdf.

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

306 Regarding the different approaches, see below: § 6.2.6.

307 2012 Cost of Cyber Crime Study: United States, Ponemon, 2012, page 7.

308 For reports on cases involving illegal content, see *Sieber*, Council of Europe Organised Crime Report 2004, page 137 *et seq.*

309 One example of the wide criminalization of illegal content is Sec. 86a German Penal Code. The provision criminalizes the use of symbols of unconstitutional parties: Section 86a: Use of Symbols of Unconstitutional Organizations:

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

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

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

312 The 2006 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "in many countries, overbroad rules in this area are abused by the powerful to limit non-traditional, dissenting, critical, or minority voices, or discussion about challenging social issues". In 2008 the Joint Declaration highlights that international organizations, including the United Nations General Assembly and Human Rights Council, should desist from the further adoption of statements supporting the idea of defamation of religions.

313 1996 Johannesburg Principles on National Security, Freedom of Expression and Access to Information.

314 The 2002 Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression points out that "defamation is not a justifiable restriction on freedom of expression; all criminal defamation laws should be abolished and replaced, where necessary, with appropriate civil defamation laws".

315 International Mechanisms for Promoting Freedom of Expression, Joint Declaration on Defamation of Religions, and Anti-Terrorism and Anti-Extremism Legislation, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, and the ACHPR (African Commission on Human and Peoples Rights) Special Rapporteur on Freedom of Expression and Access to Information, 2008.

316 See below: §§ 3.2.6 and 3.2.7.

317 In many cases, the principle of dual criminality hinders international cooperation.

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

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

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

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

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

323 Depending on the availability of broadband access.

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

325 With regard to the electronic traces that are left and the instruments needed to trace offenders, see below: § 6.5.

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

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

328 One example for this approach can be found in Sec. 184 German Criminal Code (Strafgesetzbuch):

Section 184 Dissemination of Pornographic Writings
(1) Whoever, in relation to pornographic writings (Section 11 subsection (3)):
1. offers, gives or makes them accessible to a person under eighteen years of age; […]

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

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

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

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

333 National sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

334 Regarding the principle of “dual criminality”, see below: § 6.6.2.

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

336 Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at:

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

337 Regarding the risk of detection with regard to non Internet-related acts, see: *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 63.

338 *Healy*, Child Pornography: An International Perspective, 2004, page 4.

339 *Wortley/Smallbone*, Child Pornography on the Internet, Problem-Oriented Guides for Police, USDOJ, 2006, page, 1.

340 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8 *et seq.*

341 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

342 *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 62; Rights of the Child, Commission on Human Rights, 61st session, E/CN.4/2005/78, page 8; *Healy*, Child Pornography: An International Perspective, 2004, page 5; Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 19.

343 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

344 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

345 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 8.

346 *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 41.

347 Child Pornography, CSEC World Congress Yokohama Conference, 2001, page 17.

348 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9.

349 Vienna Commitment against Child Pornography on the Internet, 1st October 1999; Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 2; *Jenkins*, Beyond Tolerance, Child Pornography on the Internet, 2001, page 49.

350 *Bloxsome/Kuhn/Pope/Voges*, The Pornography and Erotica Industry: Lack of Research and Need for a Research Agenda, Griffith University, Brisbane, Australia: 2007 International Nonprofit and Social Marketing Conference, 27-28 Sep 2007, page 196.

351 Europol, Child Abuse in relation to Trafficking in Human Beings Fact Sheet January 2006, page 1; *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1. *McCulloch*, Interpol and Crimes against Children – in Quayle/Taylor, Viewing child pornography on the Internet: Understanding the offence, managing the offender, helping the victims, 2005.

352 Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 9; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29.

353 *Eneman*, A Critical Study of ISP Filtering Child Pornography, 2006, page 1; Promotion and Protection of the Right of Children, Sale of children, child prostitution and child pornography, UN General Assembly, 51st session, A/51/456, No. 29; *Choo/Smith/McCusker*, Future directions in technology-enabled crime: 2007-09, Australian Institute of Criminology, Research and Public Policy series, No. 78, page 62.

[354] According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

[355] *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 7.

[356] See in this context, for example: *Carr*, Child Abuse, Child Pornography and the Internet, 2004, page 8.

[357] *Lanning*, Child Molesters: A Behavioral Analysis, 2001, page 64.

[358] Sexual Exploitation of Children over the Internet, Report for the use of the Committee on Energy and Commerce, US House of Representatives, 109th Congress, 2007, page 12.

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

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

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

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

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

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

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

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

[367] For more information, see: Child Pornography: Model Legislation & Global Review, 2010, page 3, available at: www.icmec.org/en_X1/icmec_publications/English__6th_Edition_FINAL_.pdf.

[368] See *Walden*, Computer Crimes and Digital Investigations, 2007, page 66.

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

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

[371] See ABA, International Guide to Combating Cybercrime, page 73.

[372] Regarding the use of electronic currencies in money-laundering activities, see: *Ehrlich*, Harvard Journal of Law & Technology, Volume 11, page 840 *et seq.*

[373] For more information, see: *Wilson*, Banking on the Net: Extending Bank Regulations to Electronic Money and Beyond., (1997) 30 Creighton Law Review 671 at 690.

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

[375] With regard to the concept see for example: *Nakamoto* (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

[376] Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf.

377 Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at:

378 See below: § 3.2.14.

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

380 See below: § 3.2.14.

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

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

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

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

385 See: Digital Terrorism & Hate 2006, available at: www.wiesenthal.com.

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

387 See: ABA International Guide to Combating Cybercrime, page 53.

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

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

390 See: *Greenberg*, A Return to Liliput: The Licra vs. Yahoo! Case and the Regulation of Online Content in the World Market, Berkeley Technology Law Journal, Vol. 18, page 1191 *et seq.*; *Van Houweling*; Enforcement of Foreign Judgements, The First Amendment, and Internet Speech: Note for the Next Yahoo! v. Licra, Michigan Journal of International Law, 2003, page 697 *et seq.*; Development in the Law, The Law of Media, Harvard Law Review, Vol. 120, page 1041.

391 See: Yahoo Inc. v. La Ligue Contre Le Racisme Et L'antisemitisme, 169 F.Supp. 2d 1181, 1192 (N.D. Cal 2001). Available at: www.courtlinkeaccess.com/DocketDirect/FShowDocket.asp?Code=21313829894194994194493893493893796151919 91.

392 *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International, 2006, page 144.

393 See: Explanatory Report to the First Additional Protocol, No. 4.

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

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

396 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology

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

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

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

399 Sec. 295-C of the Pakistan Penal Code:

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

400 Sec. 295-B of the Pakistan Penal Code:

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

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

402 www.secondlife.com.

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

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

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

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

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

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

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

410 Statista, Statistic Portal, Global Online Gambling Gross Win from 2006-2015, available at: www.statista.com/statistics/208456/global-interactive-gambling-gross-win/.

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

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

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

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

415 For more information, see: http://en.wikipedia.org/wiki/Internet_casino.

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

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

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

419 See § 5367 Internet Gambling Prohibition Enforcement Act.

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

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

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

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

424 See *Sieber*, Council of Europe Organised Crime Report 2004, page 105.

425 With regard to the challenges of investigating offences linked to anonymous services see below: § 3.2.l2.

426 See: www.wikipedia.org

427 See *Sieber*, Council of Europe Organised Crime Report 2004, page 145.

428 Similar difficulties can be identified with regard to the availability of information through the cache function of search engines and web archives, such as www.archive.org.

429 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at:

www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

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

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

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

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

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

435 2007 Sophos Report on Spam-relaying countries, available at: www.sophos.com/pressoffice/news/articles/2007/07/dirtydozjul07.html.

436 Kaspersky Security Bulletin. Spam Evolution 2013.

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

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

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

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

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

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

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

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

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

446 Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

447 See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

448 Regarding the terminology see: *Sulkowski*, Cyber-Extortion, Journal of Law, Technology & Policy, 2007, page 101 et seq.

449 *Perlroth/Wortham*, Tech Start-Ups Are Targets of Ransom Cyberattacks, NYT, 03.04.2014; *Perlroth*, Tally of Cyber Extortion Attacks on Tech Companies Grows, NYT, 19.07.2014.

450 *Ross*, BItcoin used for extortion demands, Examiner.com, 20.07.2014.

451 KPMG E-Crime Study 2013, page 7.

452 *O'Gorman/MCDonald*, Ransomware: A Growing Menace, Symantec Security Response.

453 *Wang/Ajjan*, Ransomware: Hijacking Your Data, Sophos, 2013; *Sancho/Hacquebord*, The "Police Trojan", An In-Depth Analysis, Trend Micro Research Paper, 2012.

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

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

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

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

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

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

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

461 See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, 2004, page 34 *et seq.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

477 *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

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

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

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

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

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

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

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

485 Content scrambling systems (CSS) is a digital rights management system that is used is most DVD video discs. For details about the encryption used, see: *Stevenson*, Cryptanalysis of Contents Scrambling System, available at: www.dvd-copy.com/news/cryptanalysis_of_contents_scrambling_system.htm.

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

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

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

489 *Siebel*, Council of Europe Organised Crime Report 2004, page 152.

490 See: www.golem.de/0112/17243.html.

491 Regarding the similar discussion with regard to tools used to design viruses, see below: § 2.8.4.

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

493 The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. The term originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph." linked to popular hacker naming conventions. See *Gecko*, The criminalization of Phishing and Identity Theft, Computer und Resht, 2005, 606; *Ullman*, "The Phishing Guide: Understanding & Preventing Phishing Attacks", available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information, see below: § 2.9.4.

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

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

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

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

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

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

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

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

502 Regarding the related challenges, see below.

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

504 Regarding the related automation process: § 3.2.8.

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

506 For more information, see below: § 6.2.14.

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

508 See www.ebay.com.

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

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

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

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

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

514 Regarding the criminalization of "account takeovers", see: *Gercke*, Multimedia und Recht 2004, issue 5, page XIV.

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

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

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

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

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

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

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

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

523 "Phishing" scams show a number of similarities to spam e-mails. It is likely that those organized crime groups that are involved in spam are also involved in phishing scams, as they have access to spam databases. Regarding spam, see above: § 2.6.7.

524 Regarding related trademark violations, see above: § 2.7.2.

525 For more information about phishing scams, see below: § 2.9.4.

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

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

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

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

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

531 See for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006; *Stone*, U.S. Congress looks at identity theft, International Herald Tribune, 22.03.2007.

532 See for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

533 See for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, MMR 2007, 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000.

534 *Hoar*, Identity Theft: The Crime of the New Millennium, Oregon Law Review, Vol. 80, 2001, page 1421 *et seq.*; *Levi*, Suite Revenge? The Shaping of Folk Devils and Moral Panics about White-Collar Crimes, British Journal of Criminology, 2008, page 8.

535 See: Discussion Paper Identity Crime, Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Australia, 2007, page 5.

536 See *Goodrich*, Identity Theft Awareness in North Central West Virginia, Marshall University, 2003, page 1.

[537] Identity Fraud, Prevalence and Links to Alien Illegal Activities, GAO, 2002, GAO-02-830T, page 6; *Paget,* Identity Theft, McAfee White Paper, 2007, page 6. For an overview of Internet-related phishing, see: *Emigh*, Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005, page 8 *et seq.*

[538] *McCusker*, Transnational organized cybercrime: distinguishing threat from reality, Crime Law Soc Change, Vol. 46, page 270.

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

[540] *Clarke*, Technology, Criminology and Crime Science, European Journal on Criminal Policy and Research, Vol. 10, 2004, page 55; Identity Fraud, Information on Prevalence, Cost, and Internet Impact is Limited, Briefing Report to Congressional Requesters, 1998, GAO Document: GAO/GGD-98-100BR, page 51.

[541] 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 5.

[542] 35 per cent of the overall number of cases.

[543] 2008 Identity Fraud Survey Report, Consumer Version, Javelin Strategy & Research, 200 page 6.

[544] Information Security, Agencies Report Progress, but Sensitive Data Remain at Risk, Statement of G. C. Wilshusen, Director, Information Security Issues, 2007, GAO Document: GAO-07_935T, page 4.

[545] *Elston/Stein*, International Cooperation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: www.isrcl.org/Papers/Elston%20and%20Stein.pdf.

[546] See *Koops/Leenes*, Identity Theft, Identity Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 555.

[547] *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, Bulletin of Science Technology Society, 2007, Vol. 27, 2008, page 20.

[548] See Encyclopaedia Britannica 2007.

[549] *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006, 533.

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

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

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

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

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

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

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

[557] This method is not considered as an Internet-related approach.

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

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

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

[561] The CSI Computer Crime and Security Survey 2007 analysed among other issues the economic impact of cybercrime businesses. It is based on the responses of 494 computer security practitioners from in US corporations, government agencies and financial institutions. The survey is available at: www.gocsi.com/

[562] 2013 US State of Cybercrime Survey, How Bad is the Insider Threat, Carnegie Mellon University, 2013.

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

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

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

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

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

[568] Examples is the online community Facebook, available at www.facebook.com.

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

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

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

[572] Identity Theft, Prevalence and Cost Appear to be Growing, GAO-02-363.

[573] United States Bureau of Justice Statistics, 2004, available at www.ojp.usdoj.gov/bjs/pub/pdf/it04.pdf.

[574] Press release from the Bureau of Justice Statistics, 12.12.2013, available at: www.bjs.gov/content/pub/press/vit12pr.cfm.

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

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

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

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

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

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

581 *Finkle*, 360 million newly stolen credentials on black market: cybersecurity firm, Reuters, 25.02.2014.

582 The availability of tools to commit cybercrime is one of the key challenges in the fight against cybercrime. For more information, see below: § 3.2.3.

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

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

585 See above: § 2.5.1.

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

587 DoS is an acronym for denial-of-service attack. For more information, see above: § 2.5.5.

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

589 For more details, see below: § 6.2.14.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

604 *Wilson* in CRS Report, Computer Attack and Cyberterrorism – Vulnerabilities and Policy Issues for Congress, 2003, page 4.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

623 Regarding other terrorist related activities in online games, see: *Chen/Thoms*, Cyberextremism in Web 2.0 – An Exploratory Study of International Jihadist Groups, Intelligence and Security Informatics, 2008, page 98 *et seq.*

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

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

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

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

628 The text of the final message was reported to be: "The semester begins in three more weeks. We've obtained 19 confirmations for studies in the faculty of law, the faculty of urban planning, the faculty of fine arts, and the faculty of engineering." The name of the faculties was apparently the code for different targets. For more detail, see: *Weimann*, How Modern Terrorism Uses the Internet, The Journal of International Security Affairs, Spring 2005, No. 8; *Thomas*, Al Qaeda and the Internet: The danger of "cyberplanning", 2003, available at:

http://findarticles.com/p/articles/mi_m0IBR/is_1_33/ai_99233031/pg_6; Zeller, On the Open Internet, a Web of Dark Alleys, The New York Times, 20.12.2004, available at: www.nytimes.com/2004/12/20/technology/20covert.html?pagewanted=print&position.

629 The Commission analysing the 9/11 attacks calculated that the costs for the attack could have been between USD 400 000 and 500 000. See 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, page 187. Taking into account the duration of the preparation and the number of people involved, the cost per person was relatively small. Regarding the related challenges, see also: *Weiss*, CRS Report for Congress, Terrorist Financing: The 9/11 Commission Recommendation, page 4.

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

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

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

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

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

635 *Lewis*, Assessing the Risks of Cyberterrorism, Cyberwar and Other Cyberthreats, Center for Strategic and International Studies, December 2002.

636 *Shimeall/Williams/Dunlevy*, Countering cyberwar, NATO review, Winter 2001/2002, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

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

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

639 CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

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

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

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

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

644 Regarding the discovery and functions of the computer virus, see: *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf; *Falliere/Murchu/Chien*, W32.Suxnet Dossier, Version 1.3, November 2010, Symantec, available at: www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

645 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

646 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

647 Cybersecurity Communique, American Gas Association, 2010, available at: www.aga.org/membercenter/gotocommitteepages/NGS/Documents/1011StuxnetMalware.pdf.

648 *Falliere/Murchu/Chien*, W32.Stuxnet Dossier, Symantec, November 2010, page 1; *Matrosov/Rodionov/Harley/Malcho*, Stuxnet Unter the Microscope, Rev. 1.31, 2010, available at: www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

649 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1.

650 Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

651 *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 1; Symantec W32.Stuxnet Threat and Risk Summary, available at: www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

652 See for example: *Leyden*, Lame Stuxnet Worm: "Full of Errors" says Security Consultant, The Register, 19.02.2011.

653 *Albright/Brannan/Walrond*, Did Stuxnet Take Out 1.000 Centrifuges at the Natanz Enrichment Plant?, Institute for Science and International Security, 22.12.2010; *Broad/Markoff/Sanger*, Israeli Test on Worm Called Crucial in Iran Nuclear Delay, The New York Times, 15.01.2011; *Kerr/Rollins/Theohary*, The Suxnet Computer Worm: Harbinger of an Emerging Warfare Capability, 2010, page 2; *Timmerman*, Computer Worm Shuts Down Iranian Centrifuge Plant, Newsmax, 29.11.2010.

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

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

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

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

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

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

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

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

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

663 Regarding the Stuxnet software, see: *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1.000 Centrifuges at the Nataz Enrichment Plant? Preliminary Assessment, Institute for Science and International Security, 2010.

664 *Wilson*, Information Operations and Cyberwar, Capabilities and related Policy Issues, CRS Report for Congress, RL21787, 2006; *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996..

665 *Aldrich*, The International Legal Implications of Information Warfare, INSS Occasional Paper 9, 1996.

666 *Schwartau*, Information Warfare: Chaos on the Electronic Superhighway, 1994, page 13.

667 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010.

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

669 *Sharma*, Cyberwars, A Paradigm Shift from Means to Ends, COEP, 2010..

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

671 *Libicki*, Sub Rosa Cyberwar, COEP, 2010.

672 *Myers*, Estonia removes Soviet-era war memorial after a night of violence, The New York Times, 27.04.2007; Estonia removes Soviet memorial, BBC News, 27.04.2007; *Tanner*, Violence continues over Estonia's removal of Soviet war statue, The Boston Globe, 28.04.2007.

673 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

674 *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

675 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

676 Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf

677 See: *Waterman*: Analysis: Who cybersmacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

678 See for example: *Landler/Markoff*, Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007.

679 *Shackelford*, From Nuclear War to Net War: Analogizing Cyberattacks in International Law, Berkeley Journal of International Law, Vol. 27, page 193.

680 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18-20.

681 Estonia hit by Moscow cyberwar, BBC News, 17.05.2007; *Traynor*; Russia accused of unleashing cyberwar to disable Estonia, The Guardian, 17.05.2007.

682 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

683 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 18 *et seq.*; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 8 *et seq.*

684 *Peter*, Cyberassaults on Estonia Typify a New Battle Tactic, Washington Post, 19.05.2007.

685 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 20; *Toth*, Estonia under cyberattack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

686 Regarding the background to the conflict, see: Council of Europe Parliamentary Assembly Resolution 1633 (2008), The consequences of the war between Georgia and Russia.

687 *Tikk/Kaska/Rünnimeri/Kert/Talihärm/Vihul*, Cyberaattacks Against Georgia: Legal Lessons Identified, 2008, page 4; *Hart*, Longtime Battle Lines Are Recast In Russia and Georgia's Cyberwar, Washington Post, 14.08.2008; Cybersecurity and Politically, Socially and Religiously Motivated Cyberattacks, European Union, Policy Department External Policies, 2009, page 15; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

688 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 23.

689 See for example: *Partitt,* Georgian blogger Cyxymu blames Russia for cyberattack, The Guardian, 07.08.2009.

690 *Tikk/Kaska/Vihul*, International Cyberincidents: Legal Considerations, NATO CCD COE, 2010, page 75; *Ashmore*, Impact of Alleged Russia Cyberattacks, Baltic Security & Defence Review, Vol. 11, 2009, page 10.

691 See *Walker*, Information Warfare and Neutrality, *Vanderbilt Journal of Trans-national Law* 33, 2000; *Banks*, Information War Crimes: Mitnick meets Milosevic, 2001, AU/ACSC/019/2001-04.

692 *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyberforce, Alb. Law Journal of Science and Technology, Vol. 18, page 315.

693 *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 61.

694 *Rushton*, Liberty Reserve shut down in $6bn money laundering case, The Telegraph, 28.05.2013.

695 Santora/Rashbaum/Perlroth, Online Currency Exchange Accused of Laundering $ 6 Billion, NYT.

696 Notice of Finding, Departement of the Treasury, 2013, available at: www.fincen.gov/statutes_regs/files/311--LR-NoticeofFinding-Final.pdf.

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

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

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

700 See: *Woda*, Money Laundering Techniques With Electronic Payment Systems, Information & Security, Vol. 18, 2006, page 40.

701 Regarding the related challenges, see below: § 3.2.l.

702 Regarding the fundermental concept see: Nakamoto (name reported to be used as alias), Bitcoin: A Peer-to-Peer Electronic Cash System, available at: www.bitcoin.org/bitcoin.pdf.

703 Regarding the attacks see: Cohen, Speed Bumps on the Road to Virtual Cash, NYT, 3.7.2011, available at: www.nytimes.com/2011/07/04/business/media/04link.html.

704 Regarding the basic concept of such investigation see: Following the Money 101: A Primer on Money-Trail Investigations, Coalition for International Justice, 2004, available at: www.media.ba/mcsonline/files/shared/prati_pare.pdf..

705 Regarding approaches to detect and prevent such transfers see: Financial Coalition Against Child Pornography, Report on Trends in Online Crime and Their Potential Implications for the Fight Against Commercial Child Pornography, Feb. 2011, available at: http://www.missingkids.com/en_US/documents/FCACPTrendsInOnlineCrimePaper2011.pdf

706 The costs of setting up an online casino are not significantly larger than other e-commerce businesses.

707 Regarding approaches to the criminalization of illegal gambling, see below: § 6.2.12.

[708] See: Financial Action Task Force on Money Laundering, Report on Money Laundering Typologies 2000-2001, 2001, page 2.

[709] Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

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

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

[712] The following section describes e-mail-based phishing attacks, compared to other phishing scams, which may, for example, be based on voice communications. See: *Gonsalves*, Phishers Snare Victims with VoIP, 2006, available at: www.techweb.com/wire/security/186701001.

[713] "Phishing" shows a number of similarities to spam e-mails. It is thus likely that organized crime groups that are involved in spam are also involved in phishing scams, as they make use of the same spam databases. Regarding spam, see above: § 2.6.7..

[714] Regarding related trademark violations, see above: § 2.7.2.

[715] For an overview of what phishing mails and the related spoofing websites look like, see: www.antiphishing.org/phishing_archive/phishing_archive.html.

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

[717] Anti-Phishing Working Group. For more details, see: www.antiphishing.org.

[718] Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

[719] Phishing Activitiy Trends Report, 1st Quarter 2014, WPWG, 2014.

[720] See above: § 2.8.3.

3. 与网络犯罪作斗争所面临的挑战

参考书目（节选）： *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005; *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV; *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142; *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Gercke*, The Challenge of Fighting Cybercrime, Multimedia und Recht, 2008, page 291 *et seq.*; *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2; *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19; *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*; *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001; *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Long/Skoudis/van Eijkelenborg*, Google Hacking for Penetration Testers, 2005; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago. edu/Papers/PickerCyber.200.pdf; *Putnam/Elliott,* International Responses to Cyber Crime, in Sofaer/Goodman, Transnational Dimension of Cyber Crime and Terrorism" 2001; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004; *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003; *Wallsten*, Regulation and Internet Use in Developing Countries, 2002.

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

3.1 机遇

虽然一些 ICT 服务（如匿名通信服务器或反取证工具）的发展可能会严重妨碍调查，但技术的发展亦会推动更先进调查手段的实现。

3.1.1 自动化调查概述

过去，为在犯罪嫌疑人的计算机上寻找相关证据，须主要借助手工方式。先进取证工具的发展则从根本上改变了这一状况。如今，执法机构可以使用功能日益强大的计算机系统和复杂的取证软件来加速调查和自动搜索程序。[721]

并非所有调查方法均可实现自动化。虽然根据关键字搜索非法内容可以很容易地进行，但要识别非法图片则存在更大的问题。只有当图片此前已被定级，散列值已保存在数据库中，而且所分析的图片没有进行过修改，才能成功运用基于散列值的方法。[722]

通过将嫌疑人硬盘上的文件与已知图片的信息进行比较，取证软件能够自动搜索儿童色情图片。例如，2007 年年底，主管部门发现了大量的儿童性虐待照片。违法者为了防止其身份被识别，在把图片发布在国际互联网上之前，对其脸部部分图片用数字方法进行了修改。计算机取证专家可以拆解所做的修改，并重构嫌疑人的脸部图像。[723] 尽管成功的调查清楚地展示了计算机取证的潜力，但这一案例并不能就证明在儿童色情案件调查方面取得了突破。如果犯罪嫌疑人只是简单地用白点盖住其脸部图像，那么将无法识别其身份。

3.1.2 在线服务数据的创建

如上所述，与 ICT 相关的服务目前很受欢迎。Facebook、YouTube、Instagram 和 Twitter 便是拥有数亿用户群服务的一些范例。[724]上述服务多会集中追踪用户活动。[725]这是此类公司业务模式的一部分。同时，对调查人员而言，此类数据亦颇具现实意义。若调查人员可合法获得并使用此类信息，则调查将可进入极其复杂的层面，如证实犯罪嫌疑人在实施孤掌难鸣的犯罪前曾与谁进行过沟通等。在此方面，由移动电话公司生成的地理信息亦具有同等重要意义，原因是此类数据可透露在罪案发生时犯罪嫌疑人的手机是否处于毗邻犯罪现场的某一位置。[726]

3.1.3 离线处理数字化过程中的数据创建

如今，ICT 在日常工作中已得到密集应用。视刑事调查对此类数据的授权访问和使用情况，执法机构对此类数据的采用正在日益增多。不仅新的纯数字服务（例如社交网络）会吸引用户关注并存储数据，甚至传统的离线服务亦已加入数字化阵营。例如，ICT 在邮政业务中已日益普及。[727]高速扫描仪可扫描地址，并将信息转化为电子数据。[728]美国早在 20 世纪 80 年代即已引入这种技术。[729]

据媒体报道，为配合执法调查工作，美国邮政署自 2013 年开始对所有邮件进行登记建档。[730]在 2011 年的炭疽袭击事件后，美国推出了邮件隔离控制和跟踪（MICT）项目，该项目要求对在美国邮寄的函件和包裹悉数拍照存档，以方便在罪案调查时据此开展取证工作。[731]

3.2 一般挑战

3.2.1 对信息通信技术的依赖

许多日常通信依赖信息通信技术和基于国际互联网的服务，包括 VoIP 电话或电子邮件通信。[732] 当前的信息通信技术承担着控制和管理建筑物、[733] 汽车和航空业务的作用。[734] 供能、供水以及通信服务都要依赖信息通信技术。信息通信技术有望进一步融入人们的日常生活。[735] 对信息通信技术的日益依赖使得系统与服务越来越容易受到针对关键基础设施的攻击的威胁。[736] 即使是短时

间的服务中断，也可能造成电子商务企业的巨额损失。[737] 攻击不仅会使民用通信中断；对信息通信技术的依赖对军用通信而言也是一个巨大的威胁。[738]

现有的技术基础设施存在许多弱点，如操作系统的单一性或者同质性。许多个人用户和中小型企业（SME）使用微软公司的操作系统，[739] 这使得攻击者可以专门针对这一种目标来设计有效的攻击方法。[740]

社会对信息通信技术的依赖，不仅仅限于西方国家，[741] 发展中国家同样也在防止基础设施和用户遭受网络攻击方面面临挑战。[742] 更廉价基础设施技术的发展，如 WiMAX，[743] 使发展中国家能为本国更多的人民提供互联网服务。发展中国家可以避免有些西方国家曾经犯过的错误，这些国家过于关注如何尽可能实现网络和服务的可达性，而没有在安全保护措施方面进行大的投资。美国的专家解释说，发生在爱沙尼亚的、对政府组织官方网站的成功攻击，[744] 可能仅仅是由于未采取足够的保护措施而引起的。[745] 发展中国家拥有独特的机会来较早地整合安全措施。这也许需要更大的前期投入，但从长远来看，整合安全措施的时间越晚，所需付出的代价将越大。[746]

必须制定出有效的战略来防止此类攻击，并提出应对攻击的对策，包括发展和推广技术保护手段，以及制定能够有效打击网络犯罪的、适当而充分的法律。[747]

3.2.2 用户数量

国际互联网及其服务受欢迎的程度与日俱增，到 2010 年全世界有 20 多亿国际互联网用户。[748] 计算机公司和国际互联网服务提供商正将目光聚集到发展中国家，因为这些国家拥有最大的、进一步发展的潜力。[749] 2005 年，发展中国家的国际互联网用户数量第一次超过了工业化国家，[750] 与此同时，廉价硬件以及无线接入的发展将可使更多的人们接入国际互联网。[751]

随着接入国际互联网的人数愈来愈多，攻击者及其攻击目标的数量也将增多。[752] 难以估计有多少用户在利用国际互联网从事非法活动。即使只有 0.1%的用户利用国际互联网来从事违法活动，那么违法者的总数也将超过 100 万。尽管发展中国家的国际互联网使用率较低，但推动网络安全却并不容易，原因是违法者可以从世界任何角落来实施违法行为。[753]

国际互联网用户数量的增多也给执法机构带来了难题，原因是较难以实现调查过程的自动化。虽然采用基于关键字的方法来搜索非法内容可能十分容易，但要识别非法图片是一个更大的问题。例如，只有当图片此前被定级，散列值已保存在数据库中，而且所分析的图片没有进行过修改，才能成功运用基于散列值的方法。[754]

3.2.3 设备与访问的可用性

实施计算机犯罪只需要一些基本的设备，如硬件、软件和国际互联网接入。

谈到硬件，计算机的威力仍在继续增强。[755] 为使发展中国家更广泛地使用信息通信技术，各国提出了一系列倡议。[756] 罪犯只需要使用廉价的或者二手的计算机技术就可以实施严重的网络犯罪，在这里，知识远比设备有价值得多。可用的计算机技术是新是旧，对使用这种设备来实施网络犯罪而言几乎没有任何影响。

借助专业的软件工具，可以更容易地实施网络犯罪。攻击者可以下载一些专用于定位开放端口或者破解密码保护 [757] 的软件工具。[758] 由于镜像技术和对等交换技术的存在，限制此类工具的推广应用是困难的。[759]

最后一个必不可少的要素是国际互联网接入。尽管大多数发展中国家的国际互联网接入费用[760]高于工业化国家，但发展中国家的国际互联网用户数量正在急剧增加。[761]攻击者一般不会预订一种国际互联网服务，以减少被识别的概率，他们更喜欢无需（经过验证的）注册就可以使用的服务。接入网络的一种典型方法是所谓的“驾驶攻击”。这一术语用于描述驾车游荡以寻找可接入无线网络的行为。[762]攻击者最常用的匿名网络连接方法是：公共国际互联网终端、开放（无线）网络、[763]被黑的网络以及无需注册的预付款服务。

执法机构正在采取措施，限制这种不受控制的国际互联网服务接入，以避免罪犯滥用这些服务。例如，在意大利和中国，使用公共国际互联网终端要求提供使用者的身份。[764]不过，对于这种身份要求，存在一些争议。[765]尽管对接入的限制可以防止犯罪并方便执法机构的调查，但此类规定可能阻碍信息社会和电子商务的发展。[766]

有人认为，对国际互联网接入的这种限制有可能侵犯人权。[767]例如，欧洲法庭在许多有关广泛的案件中裁定，自由表达的权利不仅仅适用于信息的内容，也适用于发射或接收的方法。在瑞士Autronic v.公司的案件中[768]，法庭坚称，由于任何强加于接入方法上的限制都将干扰接收和传送信息的权利，因此有必要作出进一步的解释。如果这些原则应用于对国际互联网接入的潜在限制，那么此类法律措施可能造成对人权的侵犯。

3.2.4 信息的可用性

国际互联网上拥有数百万个网页，[769]上面都是一些最新的信息。任何一个公布或维护一个网页的人都可以参与。维基百科（Wikipedia）就是由用户自己产生的平台的一个成功例子，[770]它是一部任何人都可以发布信息的在线百科全书。[771]

国际互联网的成功还取决于强大的搜索引擎，它们可以使用户在数秒钟内搜索到数百万个网页。这一技术可同时用于合法和犯罪的目的。“谷歌黑客”或者“谷歌剁客”指的是使用复杂的搜索引擎查询来过滤大量的搜索结果，以寻找与计算机安全问题相关的信息。例如，攻击者可能着眼于搜索不安全的密码保护系统。[772]报告强调了非法使用搜索引擎的风险。[773]打算进行攻击的攻击者，可以在国际互联网上找到关于如何使用能够在普通超市中买到的化学物质来制造炸弹的详细信息。[774]尽管此类信息即使在国际互联网问世之前同样也可以获得，但不管怎样，以前要获得此类信息要困难得多。如今，任何国际互联网用户都可以接触到此类指南。

罪犯还可以使用搜索引擎来分析攻击目标。[775]在调查恐怖组织成员的过程中，调查人员发现了一份培训手册，这突显了国际互联网在收集可能的目标方面能够发挥巨大的作用。[776]使用搜索引擎，攻击者能够收集到公开的有用信息（如公共建筑物的建筑规划），这将有助于其准备攻击行动。有报道指出，攻击驻阿富汗英军的武装分子就使用了来自谷歌地球（Google Earth）的卫星图片。[777]

3.2.5 控制机制的缺失

所有的大规模通信网络，从用于语音电话的电话网络到国际互联网，都需要中央控制和技术标准，以确保操作性。当前关于国际互联网管理问题的讨论表明，与国家甚至跨国通信基础设施相比，国际互联网并没有什么不同。[778]国际互联网也需要受到法律的制约，立法者和执法机构已经开始制定一些法律标准，以便对国际互联网实施一定程度的中央控制。

国际互联网最初是设计为一种军事网络，[779]它基于一种分散的网络体系结构，旨在当网络的组成部分受到了攻击时，保持主要功能的完整和有效。结果是，国际互联网的网络基础设施对外部的控制意图具有抵抗性。最初的设计并非为了便于犯罪调查或者防止来自网络内部的攻击。

如今，国际互联网在民用服务中的使用越来越广泛。随着从军用转向民用，对控制手段的需求特性也发生了变化。由于网络基于为军事用途而设计的协议，因此并不存在这些中央控制手段，而且如果不对网络进行重大的重新设计，是难以追溯式地来实施控制的。缺少控制手段使得对网络犯罪的调查变得十分困难。[780]

由于缺乏控制手段而引发问题的一个例子是使用加密匿名通信服务[781]的用户可以绕过过滤技术。[782]如果接入提供商拦阻含有非法内容（如儿童色情）的某些网站，用户一般将无法访问它们。但是，如果用户在他们与中央服务器之间使用匿名通信服务器加密通信，那么就可以避开对非法内容的拦阻。在这种情况下，提供商可能无法拦阻这些请求，原因是访问提供者也无法打开作为加密消息发送的请求。

3.2.6 国际影响

许多数据传送过程会影响到多个国家。[783]如果直接链路被临时阻断，那么用于国际互联网数据传送的协议将基于最理想的路径。[784]甚至在发起国中的国内传送过程受到限制时，数据也可以离开这个国家，并传送到境外的路由器上，并重新导回到其最终目的地所在的国家。[785]此外，许多国际互联网服务基于国外的服务，[786]例如，托管服务提供商可以基于一个国家的硬件来在另一个国家提供网络空间租用服务。[787]

如果攻击者和攻击对象位于不同的国家，那么网络犯罪调查需要所有受影响国家的执法机构的合作。[788]国家主权不允许未经当地主管部门的同意就在别国的领土范围内开展调查。[789]网络犯罪调查需要所有相关国家主管部门的支持与参与。

在应对网络犯罪时，难以根据传统的法律互助原则来开展合作。与国外执法机构协调所需的正式要求以及所需的时间，常常阻碍网络犯罪调查的开展。[790]调查常常要在非常短的时间周期内进行。[791]跟踪违法行为所需的关键数据常常会在很短的时间后便会被删去。这样短的调查时间是有问题的，原因是传统的法律互助体系常常需要花时间来组织。[792]如果调查中的违法行为在某个相关国家不被认为是有罪的[793]，那么双重犯罪原则[794]也会带来一些难题。攻击者可能故意将第三国纳入其攻击范围，以增加网络犯罪调查的难度。[795]

罪犯可能故意选择本国之外的目标，并且从那些对网络犯罪立法不够严格的国家开始行动。[796]与网络犯罪有关的法律协调以及国际合作，将有助于应对这些问题。在网络犯罪调查中促进国际合作有两种方法：一是八国集团的 24/7 网络；[797] 二是欧洲理事会《网络犯罪公约》中与国际合作有关的规定。[798]

3.2.7 现场外的远程犯罪

罪犯不必出现在目标对象所在的同一地点。由于罪犯的位置可与犯罪现场完全不同，因此许多网络违法行为是跨国的。国际性的网络犯罪行为要耗费大量的精力和时间。网络罪犯力求避开那些具有严格网络犯罪立法的国家。[799]

在与网络犯罪作斗争的过程中，防止“安全避风港”的出现是其中的一项关键挑战。[800]一旦存在“安全避风港”，违法者将利用它们来阻止犯罪调查。尚未实施网络犯罪法律的发展中国家可能变得容易受到攻击，原因是罪犯可选择以这些国家作为基地，以避免遭到起诉。由于违法者处在法律不健全的国家中，因此难以阻止会影响到全球受害者的严重违法行为。这可给某些特定的国家施加一定的压力，迫使它们考虑通过法律来制裁网络犯罪。这方面的一个例子是：2000 年，一位犯罪嫌疑人在菲律宾开发出了“爱虫”计算机蠕虫病毒，[801]该病毒感染了全世界数百万台计算机。[802]但由于当时的菲律宾尚未对研发和传播恶意软件的行为做适当的定罪，因而使得当地的调查工作受

阻。[803] 另一个例子是尼日利亚，它曾受到国际压力，被迫针对借助电子邮件进行的金融骗局采取行动。

3.2.8 自动化

信息通信技术的最大优势之一是能够自动执行某些过程。自动化的若干主要优势是它加速了过程的进展、扩大了过程的范围和影响及限制了人类的参与。

自动化减少了对成本密集的人力的需求，使提供商能够以更低的价格来提供服务。[804] 攻击者可以利用自动化来扩大其犯罪活动的规模 — 数百万条主动发出的垃圾邮件 [805] 短信可以借助自动化方式发出。[806] 如今，黑客攻击常常也是自动进行的，[807] 每天有多达 8000 万次的黑客攻击 [808] 是因使用软件工具而自动进行的，[809] 它们可以在数小时内对数千个计算机系统实施攻击。[810] 借助自动化过程，攻击者可以通过设计骗局来牟取暴利，这些骗局基于数量巨大的攻击，每个受害者蒙受的损失相对较小。[811] 单个受害者的损失越小，受害者就越有可能不会报告自己所遭受的攻击。

攻击自动化对发展中国家的影响尤其显著。由于它们的资源有限，因此相比工业化国家，发展中国家因垃圾邮件而造成的问题将更加严重。[812] 通过自动化来实施的犯罪数量越大，对全世界执法机构的挑战就越严峻，原因是在其管辖范围内不得不需要准备面对更多的受害者。

3.2.9 资源

目前进入市场的现代计算机系统的功能非常强大，可以用于扩大犯罪活动的规模。但并不是仅仅因单个用户计算机性能的增强而给调查带来了诸多问题，[813] 网络容量的增大也是一个主要问题。

最近的一个攻击案例是对爱沙尼亚政府网站的攻击。[814] 对这些攻击的分析表明，它们是通过一个“僵尸网络”[815] 上的成千上万台计算机来实施的，或者是在外部控制下运行程序的一组受到危害的计算机来实施的。[816] 在大多数情况下，受到恶意软件感染的计算机都安装了一些工具，使作案者可以对其实施控制。僵尸网络用于收集与目标有关的信息，或者实施高水平的攻击。[817]

最近几年，僵尸网络已成为网络安全的一个严重威胁。[818] 僵尸网络的规模可大可小，小到几台计算机，大到 100 多万台计算机。[819] 当前的分析表明，在连接到国际互联网的所有计算机中，有多达四分之一的计算机可能被恶意软件感染，使之成为僵尸网络的一部分。[820] 僵尸网络可以用于各种犯罪活动，包括发起拒绝服务攻击、[821] 发送垃圾邮件、[822] 黑客攻击；以及交换受版权保护的文件。

僵尸网络为攻击者提供了诸多优势。它们增强了罪犯的计算机与网络能力。使用成千上万个计算机系统，罪犯可以攻击其他遥不可及的计算机系统，只需少量的计算机来引导攻击行动。[823] 僵尸网络还使执法机构更难跟踪最初的攻击者，原因是最初的跟踪线索只导向僵尸网络的成员。由于罪犯控制着更为强大的计算机系统与网络，因此调查部门的计算机系统与网络的能力与那些处在罪犯控制之下的计算机系统与网络的能力之间的差距正变得越来越大。

3.2.10 数据交换处理的速度

在国与国之间传送电子邮件只需几秒钟的时间。这么短的时间也是国际互联网取得成功的理由之一，电子邮件大大缩短了物理传送消息的时间。不过，如此迅速的数据交换也给执法机构带来了困难，因为几乎没有给它们留下多少调查或收集证据的时间。传统的调查通常需要花费更长的时间。[824]

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

电子邮件还展示了可以立即付诸使用的即时反应工具的重要性。为了跟踪和识别犯罪嫌疑人，调查人员通常需要访问一些数据，而这些数据在传输之后可能很快就被删去。[825] 调查机构要求在很短的时间内作出反应，这对于成功的调查至关重要。没有使调查人员能够迅速作出反应且阻止数据被删除的恰当的法律和工具，是无法有效地与网络犯罪作斗争的。[826]

“快速冻结程序” [827] 以及 24/7 网络点 [828] 是可以提高调查效率的工具的例子。针对数据保留的立法还着眼于增加执法机构进行调查时可用的时间裕量。如果在一段时间内保留了跟踪违法者所需的数据，那么执法机构成功识别犯罪嫌疑人的机率就会更大。

3.2.11 发展速度

国际互联网不断在发展。图形用户接口（WWW [829] ）的问世标志着它开始迅速扩展，原因是过去一些基于命令的服务不够用户友好。WWW 的问世还使一些新的应用以及新的犯罪活动 [830] 成为可能。在这方面，执法机构正在努力追赶。进一步的发展仍在继续，主要表现在在线游戏以及网际协议语音服务（VoIP）通信。

在线游戏更为流行，但目前尚不清楚执法机构是否能够成功调查和起诉在这一虚拟世界中实施的违法犯罪活动。[831]

从传统的语音电话到国际互联网电话的转变，也对执法机构提出了新的挑战。由执法机构开发的、用于截获传统手机通信的方法和程序，通常无法用于 VoIP 通信。对传统语音电话的截获通常要通过电信提供商来进行。将相同的原则运用于 VoIP，执法机构将需要通过 ISP 以及提供 VoIP 服务的服务提供商来进行。不过，如果服务基于对等技术，那么服务提供商一般无法截获通信，原因是相关的数据是在通信各方之间直接传输的。[832] 因此，需要一些新的技术。[833]

采用新的网络技术的硬件设备也正在迅速发展中。最新的家庭娱乐系统将电视转变成了国际互联网接入点，而最新的移动式手持设备可以存储数据，并且能够通过无线网络连接到国际互联网。[834] 容量超过 1 GB 的 USB（通用串行总线）存储设备已经集成到手表、钢笔和小刀中。执法机构需要在其工作中考虑到这些发展 — 不断对网络犯罪调查人员进行培训，使他们能够及时掌握最新技术，并能够识别相关的硬件以及任何需要掌握的特殊设备，这是一项至关重要的工作。

另一个挑战是无线接入点的使用。无线国际互联网接入在发展中国家的扩张是一个机会，对执法机构而言，则是一个挑战。[835] 如果违法者使用不需要注册的无线接入点，那么执法机构将更难跟踪违法者，原因是调查只能引向接入点。

3.2.12 匿名通信

确定通信来源通常是网络犯罪调查的一大要素。然而网络的分布特性以及模糊了来源的某些国际互联网服务的提供，使违法者难以识别。[836] 匿名通信的可能性或者只是某种服务的附带服务，或者是出于避免用户劣势的考虑而提供的。[837] 注意到来源的不确定性，对于避免得出错误结论至关重要。[838] 此类服务的例子（甚至可以将它们结合起来）包括：

- 公共国际互联网终端（例如，在机场航站楼或网吧）；[839]
- 网络地址转换（NAT）装置和虚拟专用网（VPN）；[840]

- 无线网络；[841]
- 无需注册的预付费移动服务；
- 无需注册的、为主页提供的存储容量；
- 匿名通信服务器；[842]
- 匿名信件转发器。[843]

例如，违法者可以通过使用伪造的电子邮件地址来隐藏其身份。[844] 许多提供商提供免费的电子邮件地址。即使是应当输入个人信息的地方，也可能不需要进行验证，因此，用户可以在不泄露其身份的情况下注册电子邮件地址。例如，如果用户希望加入政治话题讨论团体而不泄露其身份，那么匿名的电子邮件地址就是有用的。匿名通信可能导致反社会行为，但它们也使用户能够更加自由地开展活动。[845]

考虑到用户留下的各种线索，显示了需要利用一些手段来防止用户描绘特征剖面的行为。[846] 因此，世界各国和组织都支持匿名使用国际互联网电子邮件服务的原则，例如，《欧盟关于隐私与电子通信的指令》就明确表达了这一原则。[847] 用法律手段来保护用户隐私的一个例子可以在《欧盟关于数据保护的规定》第 37 条中找到。[848] 不过，一些国家正通过实施法律限制来应对匿名通信的挑战 [849] 例如，意大利要求公共国际互联网接入提供商在用户开始使用服务之前辨别其身份。[850]

这些措施旨在帮助执法机构识别犯罪嫌疑人，但它们易于被犯罪嫌疑人避开。作案者可以使用来自无需注册国家的、未受保护的无线网络或者 SIM 卡。目前尚不明确的是，在网络安全战略中，对匿名通信和匿名接入国际互联网的限制是否应该发挥更加重要的作用。[851]

3.2.13 失效的传统调查工具

网络犯罪的侦办，需要能够使主管当局开展调查的互联网专用工具。[852] 在这种情况下，刑事诉讼所需的嫌犯识别和证据采集的工具，则具有至关重要的作用。[853] 这些工具可能与无关计算机技术的传统恐怖分子调查所用的工具相同。但对于数量日增的互联网相关案件而言，传统的侦察工具已不足以识别嫌犯，而截获互联网协议语音（VoIP）通信就是一个例子。[854] 在最近的几十年间，各国研发了可截获陆线和移动电话通信的监听刑侦工具。[855] 截获传统语音呼叫，通常是通过电信业务提供商进行的。[856] 如对 VoIP 也采用相同的原则，执法机构将通过互联网业务提供商（ISP）和 VoIP 业务提供商开展工作。但倘若业务是基于对等技术的，业务提供商一般无法截获通信，因为相关数据是直接传送给通信合作伙伴的。[857] 因而有必要制定具有相关法律工具的新型技术解决方案。

3.2.14 加密技术

另一个可使网络犯罪调查变得复杂的因素是加密技术，[858] 它使未获授权人员无法访问信息，是与网络犯罪作斗争过程中一种重要的技术解决方案。[859] 加密是利用算法将纯文本变为隐晦格式的技术，[860] 同匿名技术一样，加密也不是新事物，[861] 但计算机技术改变了这一领域。虽然长期以来一直处于保密状态，但在互连互通的环境中，这种保密状态就难为维持了。[862]

由于易于使用的软件工具的普及和操作系统[863] 中加密技术的融合，如今，只需轻轻点击一下鼠标，就可以对计算机数据进行加密，从而增加了执法机构面对加密资料的机会。[864] 现有的各种软件产品可使用户保护其文件免受未经授权的访问。[865] 尚不明确的是，违法者已经在多大程度上使用加密技术来掩盖其犯罪活动。[866] 一项关于儿童色情的调查表明，只有 6%的被抓获的儿童色情资料持

有者使用了加密技术，[867] 但专家强调，在网络犯罪案件中，存在着越来越多使用加密技术的威胁。[868]

目前有各种各样可用来保护加密数据的技术战略，也有多种使这些程序实现自动化的可用软件工具。[869] 我们既有文件加密软件工具弱点分析[870] 战略，也有密码短语[871] 搜寻和常用密码深度战略，[872] 还有针对复杂和长时间强为攻击战略。“强为攻击”一词被用于说明通过测试每个可能的组合寻找密码的过程。[873] 根据加密技术和密钥规模的情况，这一破译程序也许需要花费几十年的时间。[874] 例如，如果攻击者使用一个拥有 20 位密码的加密软件，那么密钥空间的规模大约为 100 万。使用当前每秒能够处理 100 万次操作的计算机，那么破解这一密码可以在不到 1 秒钟的时间内完成。不过，如果攻击者使用一个拥有 40 位密码的加密软件，那么可能需要花费两周的时间才能将其破解。[875] 例如，《华尔街日报》于 2002 年成功破译了在基地组织计算机中发现的 40 位加密文件。[876] 如果攻击者使用 56 位的密码，那么单独一台计算机可能需要花费 2285 年的时间才能将其破解。如果攻击者使用 128 位的密码，那么即使有十亿台计算机系统专用于解密，那么也需要花上数万亿年的时间才能将其破解。[877] 流行的最新版的加密软件 PGP，允许采用 1024 位密码。

当前的加密软件远不只仅对单个文件进行加密。例如，最新版的微软操作系统能够对整个硬盘进行加密。[878] 用户可以容易地安装加密软件。尽管某些计算机取证专家认为，这一功能并不会威胁到他们，[879] 但任何用户都可以广泛使用这一技术可能导致对加密技术的更广泛应用。还有一些工具可用来对通信进行加密 — 例如，电子邮件和电话呼叫 [880] 都可以使用 VoIP [881] 来发送。使用加密的 VoIP 技术，攻击者可以保护语音谈话免被截获。[882]

这些技术也可结合使用。运用软件工具，攻击者可以对消息进行加密，然后以图片或图像的形式交换它们 — 这种技术称为加密图形技术。[883] 对调查机构而言，难以区别究竟是无害的度假照片交换，还是带有加密、隐藏消息的图片交换。[884]

加密技术的可用性以及罪犯对加密技术的使用，对执法机构而言是一个挑战。解决这一问题的各种各样法律方法目前正在讨论中，[885] 包括：软件开发商为执法机构安装一个后门的潜在义务；限制密钥的强度；在犯罪调查情况下透露密钥的义务。[886] 但加密技术不仅仅可被攻击者使用 — 此类技术也可以以各种各样的方式用于法律目的。不恰当使用加密技术，可能难以对敏感信息实现保护。考虑到日益增多的攻击数量，[887] 自我保护是网络安全的一个重要因素。

3.2.15 小结

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

3.3 法律挑战

3.3.1 国际刑法起草方面的挑战

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

历史上，与计算机有关的服务或者与国际互联网有关的技术的引入，都会在技术引入后很快带来新的犯罪形式。计算机网络发展的一个例子是 20 世纪 70 年代 — 这之后不久，就出现了第一起未经授权访问计算机网络的案例。[888] 同样，在 20 世纪 80 年代个人计算机引入后不久，就发生了第一起软件违法行为，当时，这些系统用于复制软件产品。

更新国家刑法以起诉新的在线网络犯罪形式需要花费时间 — 有些国家尚未结束这一调整过程。一直以来依据国家刑法来判定违法行为的罪行，这一作法需要进行评审和更新。例如，数字信息必须具备与传统签名和打印资料相当的效用。[889] 若不综合考虑与网络犯罪有关的违法行为，网络犯罪行为将无法受到起诉。

对国家刑法体系而言，主要的挑战是：意识到潜在的新技术滥用与需要对国家刑法进行修改之间存在一个时延。这一挑战随着网络创新速度的加快，依然是一个切实相关的问题。许多国家正致力于赶上法律调整的步伐。[890] 一般地，调整过程分为三个步骤：调整国家法律、发现刑法缺陷和起草新的立法。

调整国家法律必须首先意识到新技术的滥用问题

在国家执法机构内部，需要设立专门的部门，这些部门有资格来调查潜在的网络犯罪。成立计算机应急响应小组（CERT）、[891] 计算机事件响应小组（CIRT）、计算机安全事件响应小组（CSIRT）以及其他研究机构等，已使这一状况得到改善。

发现刑法缺陷

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

起草新的立法

根据经验，由于网络技术的迅猛发展及其复杂的结构，如果不进行国际合作，要求国家主管部门起草完成针对网络犯罪的法律可能是困难的。[892] 各国单独起草网络犯罪法律可能导致巨大的复制效应，造成资源浪费，此外，起草机构也需要密切跟踪国际标准和战略的发展。没有国际上对各国刑法规定的协调，各国法律上的不一致性或不兼容性会使与跨国网络犯罪的斗争变得异常困难。因此，协调不同国家刑法的国际努力正变得日益重要。[893] 国家法律可以极大地受益于其他国家的经验和国际专家的法律建议。

3.3.2 新的违法行为

在大多数情况下，使用信息通信技术实施的犯罪并非新鲜事物，但经过修改的骗局将在网上实施。其中一个例子是欺诈 — 攻击者向受害者写信，意在误导受害者，与出于同样目的向受害者发送电子邮件，本质上没有太大区别。[894] 如果欺诈已经认定是一种犯罪行为，那么为起诉此类行为就不一定非要对国家法律进行调整。

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

除了针对臭名昭著的骗局对法律进行修改之外，立法者还必须不断地对新的和发展中的网络犯罪类型进行分析，以确保能对其罪行作出有效判定。在所有国家都尚未定罪的一个网络犯罪例子是，在计算机和在线游戏中的盗窃和欺诈。[895] 很长时间以来，关于在线游戏的讨论重点聚焦于未成年人的保护问题（例如，对年龄进行验证的要求）和非法内容（例如，在在线游戏“Second Life”中对儿童色情内容的访问）。[896] 新的犯罪行为仍在不断涌现。在线游戏中的虚拟货币也可能被“偷

盗”，并在拍卖平台中进行交易。[897] 有些虚拟货币比照现实货币具有一定的价值（根据交易率），这给网络犯罪增加了“真实感”。[898] 此类违法行为可能不会在所有国家遭到起诉。为了防止违法者找到安全的避风港，密切关注世界范围的发展状况是至关重要的。

3.3.3 越来越多的信息通信技术的应用与新的调查手段的需求

在准备和实施其违法行为过程中，违法者以各种各样的方式来使用信息通信技术。[899] 执法机构需要适当的手段来调查潜在的犯罪行为。有些手段（如数据保留 [900] ）可能侵犯到清白的国际互联网用户的权利。[901] 如果犯罪行为的严重程度与这种侵犯的程度不成比例，那么调查手段的使用可能就是非合理的或者是非法的。结果是，在许多国家，目前尚未引入能够改进网络犯罪调查工作的手段。

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

3.3.4 开发数字证据程序

特别是由于相比保存物理文件而言，低得多的成本，[902] 因此数字文件的数量正与日俱增。[903] 数字化和信息通信技术的新兴应用，对与证据收集及其在法庭上使用有关的程序产生了巨大影响。[904] 发展的一个结果是，引入数字证据作为一种新的证据源。[905] 它被定义为使用计算机技术存储或传输的任何数据，用于支持推测一种违法行为是如何产生的。[906] 对数字证据的处理也伴随着一些独特的挑战，并需要特定的程序。[907] 其中最难的一个问题是保持数字证据的完整性。[908] 数字数据是极为脆弱的，非常容易被删去 [909] 或被修改。对保存在系统存储器 RAM 中的信息而言更是如此，当系统关机时，这些信息会被自动删去，[910] 因此，需要特殊的保存技术。[911] 此外，新的发展对数字证据的处理产生了极大的影响。一个例子是云计算。过去，调查者能够重点关注犯罪嫌疑人的前提条件，并搜寻计算机数据。如今，他们需要考虑这些数字信息可能保存在国外，并且必要的话，只能远程访问之。[912]

数字证据在网络犯罪调查的各个阶段都发挥着重要作用。一般可将数字证据处理分为四个阶段：[913] 首先是相关证据识别阶段，[914] 其后是证据收集和保留阶段。[915] 第三阶段涉及对计算机技术和数字证据的分析，最后是需要在法庭上出示证据。

除了涉及在法庭上出示证据的相关程序，收集数字证据的方法需要特别加以关注。数字证据的收集与计算机取证相关联。“计算机取证”这一术语指的是，本着搜索数字证据的目的，对信息技术设备进行系统的分析。[916] 对于以数字格式保存的数据仍在不断增长这一事实，则突显了此类调查面临的逻辑上的挑战。[917] 自动执行取证程序的方法发挥着重要作用，[918] 例如，使用基于散列值的方法来搜索已知的儿童色情图片，[919] 或者借助关键字进行搜索。[920]

例如，计算机取证可以根据具体调查的要求，包括以下步骤：分析嫌疑犯所用的硬件和软件，[921] 在确定相关证据中为调查者提供支持，[922] 恢复被删除的文件，[923] 破解文件 [924] 以及通过分析通信流量数据来识别国际互联网用户。[925]

721 See: *Giordano/Maciag*, Cyber Forensics: A Military Operations Perspective, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04843F3-99E5-632B-FF420389C0633B1B.pdf ; *Reith*, An Examination of Digital Forensic Models, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-

98F94F16AF57232D.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

722 Regarding hash-value based searches for illegal content, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 546 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

723 For more information about the case, see: Interpol in Appeal to find Paedophile Suspect, The New York Times, 09.10.2007, available at: www.nytimes.com/2007/10/09/world/europe/09briefs-pedophile.html?_r=1&oref=slogin; as well as the information provided on the Interpol website, available at: www.interpol.int/Public/THB/vico/Default.asp

724 In 2014 Facebook alone reported 829 million daily active users and 1.32 billion monthly active user. Source: http://newsroom.fb.com/company-info/.

725 See for example: *Chaabane/Kaafar/Boreli*, Big Friend is Watching You: Analyzing Online Social networks Tracking Capabilities, Proceedings of the 2012 ACM workshop on online social networks, page 7 et seq.

726 See in this regard: *Daniel*, Cellular Location Evidence for Legal Professionals, 2014.

727 Regarding the development see: The United States Postal Service – An American History 1775-2006, available online: https://about.usps.com/publications/pub100/pub100_042.htm.

728 Regarding the process see: *Rlamondon/Srihari*, On-Line and Off-Line Handwriting Recognition: A Comprehensive Survey, ICC Transactions on pattern Analysis and machine Intelligence, Vol. 22, No.1, 2000, page 63 et seq.

729 The United States Postal Service – An American History 1775-2006, available online: https://about.usps.com/publications/pub100/pub100_042.htm.

730 *Nixon*, Postal Service Confirms Photographing all U.S. Mail, NYT, 02.08.2013.

731 *Nixon*, Postal Service Confirms Photographing all U.S. Mail, NYT, 02.08.2013.

732 It was reported that the United States Department of Defense had to shut down their e-mail system after a hacking attack. See: www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

733 Examples include the control of air-conditioning, access and surveillance systems, as well as the control of elevators and doors.

734 See *Goodman*, The Civil Aviation Analogy – International Cooperation to Protect Civil Aviation Against Cyber Crime and Terrorism in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 69, available at: http://media.hoover.org/documents/0817999825_69.pdf.

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

736 Regarding the impact of attacks, see: *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 3, available at: http://media.hoover.org/documents/0817999825_1.pdf.

737 A demonstration of the impact of even short interruptions to Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the worm affected computers running versions of Microsoft's Windows operating system. As a result of the worm, a number of services were interrupted. Among them were the US airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm, whilst the electronic mapping services of the British Coastguard were disabled for a few hours. See Heise News, 04.01.2005, available at: www.heise.de/newsticker/meldung/54746; BBC News, "Sasser net worm affects millions", 04.05.2004, available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

738 *Shimeall/Williams/Dunlevy*, Countering cyber war, NATO review, Winter 2001/2002, page 16, available at: www.cert.org/archive/pdf/counter_cyberwar.pdf.

739 One analysis by "Red Sheriff" in 2002 stated that more than 90 per cent of users worldwide use Microsoft`s operating systems (source: www.tecchannel.de – 20.09.2002).

740 Regarding the discussion on the effect of the monoculture of operating systems on cybersecurity, see *Picker*, Cyber Security: Of Heterogeneity and Autarky, available at: http://picker.uchicago.edu/Papers/PickerCyber.200.pdf; Warning: Microsoft 'Monoculture', Associated Press, 15.02.2004, available at www.wired.com/news/privacy/0,1848,62307,00.html; *Geer and others*, CyberInsecurity: The Cost of Monopoly, available at: http://cryptome.org/cyberinsecurity.htm.

741 With regard to the effect of spam on developing countries, see: Spam issues in developing countries, 2005, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

742 Regarding the integration of developing countries in the protection of network infrastructure, see: Chairman's Report on ITU Workshop On creating trust in Critical Network Infrastructures, available at: www.itu.int/osg/spu/ni/security/docs/cni.10.pdf; World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

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

744 Regarding the attack, see: *Toth*, Estonia under cyberattack, available at: www.cert.hu/dmdocuments/Estonia_attack2.pdf

745 See: *Waterman*: Analysis: Who cyber smacked Estonia, United Press International 2007, available at: www.upi.com/Security_Terrorism/Analysis/2007/06/11/analysis_who_cyber_smacked_estonia/2683/.

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

747 See below: § 4.

748 According to ITU, there were over 2 billion Internet users by the end of 2010, of which 1.2 billion in developing countries. For more information see: ITU ICT Facts and Figures 2010, page 3, available at: www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf.

749 See *Wallsten*, Regulation and Internet Use in Developing Countries, 2002, page 2.

750 See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

751 An example for new technology in this area is WiMAX (Worldwide Interoperability for Microwave Access), a standards-based wireless technology that provides broadband connections over long distances. Each WiMAX node could enable high-speed Internet connectivity in a radius of up to 50 km. For more information, see: The WiMAX Forum at www.wimaxforum.org; *Andrews, Ghosh, Rias*, "Fundamentals of WiMAX: Understanding Broadband Wireless Networking"; *Nuaymi*, WiMAX, Technology for Broadband Wireless Access.

752 Regarding the necessary steps to improve cybersecurity, see: World Information Society Report 2007, page 95, available at: www.itu.int/osg/spu/publications/worldinformationsociety/2007/WISR07_full-free.pdf.

753 The fact that the offenders are not only based in western countries is proven by current analysis that suggests for example that an increasing number of phishing websites are hosted in developing countries. For more details, see: Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf. Regarding phishing, see above: § 2.9.4.

754 Regarding hash-value based searches, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233.

755 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law). For more information, see *Moore*, Cramming more components onto integrated circuits, Electronics, Volume 38, Number 8, 1965, available at: ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf; *Stokes*, Understanding Moore's Law, available at: http://arstechnica.com/articles/paedia/cpu/moore.ars/.

756 "World Information Society Report 2007", ITU, Geneva, available at: www.itu.int/wisr/

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

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

759 In order to limit the availability of such tools, some countries criminalize their production and offer. An example of such a provision can be found in Art. 6 of the Council of Europe Convention on Cybercrime. See below: § 6.2.15.

760 Regarding the costs, see: The World Information Society Report, 2007, available at: www.itu.int/wisr/

761 See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

762 For more information, see: *Ryan*, War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue3/v9i3_a07-Ryan.pdf

763 With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

764 One example of an approach to restrict the use of public terminals for criminal offences is Art. 7 of the Italian Decree-Law No. 144. Decree-Law 27 July 2005, No. 144 – "Urgent measures for combating international terrorism". For more information about the Decree-Law, see for example the article "Privacy and data retention policies in selected countries", available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

765 See below: § 6.5.13.

766 Regarding the impact of censorship and control, see: *Burnheim*, The right to communicate, The Internet in Africa, 1999, available at: www.article19.org/pdfs/publications/africa-internet.pdf

767 Regarding the question whether access to the Internet is a human right, see: *Hick/Halpin/Hoskins*, Human Rights and the Internet, 2000; Regarding the declaration of Internet Access as a human right in Estonia, see: Information and Communications Technology, in UNDP Annual Report 2001, page 12, available at: www.undp.org/dpa/annualreport2001/arinfocom.pdf; Background Paper on Freedom of Expression and Internet Regulation, 2001, available at: www.article19.org/pdfs/publications/freedom-of-expression-and-internet-regulation.pdf.

768 Autronic v. Switzerland, Application No. 12726/87, Judgement of 22 May 1990, para. 47. Summary available at: http://sim.law.uu.nl/sim/caselaw/Hof.nsf/2422ec00f1ace923c1256681002b47f1/cd1bcbf61104580ec1256640004c1d0b?OpenDocument.

769 The Internet Systems Consortium identified 490 million Domains (not webpages). See the Internet Domain Survey, July 2007, available at: www.isc.org/index.pl?/ops/ds/reports/2007-07/; The Internet monitoring company Netcraft reported in August 2007 a total of nearly 130 million websites at: http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html.

770 http://www.wikipedia.org

771 In the future development of the Internet, information provided by users will become even more important. "User generated content" is a key trend among the latest developments shaping the Internet. For more information, see: *O'Reilly*, What Is Web 2.0 – Design Patterns and Business Models for the Next Generation of Software, 2005, available at: www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html.

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

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

774 One example is the "Terrorist Handbook" – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

775 See *Thomas*, Al Qaeda and the Internet: The Danger of 'Cyberplanning' Parameters 2003, page 112 *et seq.*, available at: www.iwar.org.uk/cyberterror/resources/cyberplanning/thomas.pdf; *Brown/Carlyle/Salmerón/Wood*, "Defending Critical Infrastructure", Interfaces, Vol. 36, No. 6, page 530, available at: www.nps.navy.mil/orfacpag/resumePages/Wood-pubs/defending_critical_infrastructure.pdf.

776 "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80 per cent of all information required about the enemy". Reports vary as to the source of the quotation: The British High Commissioner Paul Boateng mentioned in a speech in 2007 that the quote was "contained in the Al Qaeda training manual that was recovered from a safe house in Manchester" (see: *Boateng*, The role of the media in multicultural and multifaith societies, 2007, available at: www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=112556

0437610&a=KArticle&aid=1171452755624. The United States Department of Defence reported that the quote was taken from an Al Qaeda Training Manual recovered in Afghanistan (see: www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html). Regarding the availability of sensitive information on websites, see: *Knezo*, "Sensitive but Unclassified" Information and Other Controls: Policy & Options for Scientific and Technical Information, 2006, page 24, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-8704:1.

777 See Telegraph.co.uk, news from 13 January 2007.

778 See for example, *Sadowsky/Zambrano/Dandjinou*, Internet Governance: A Discussion Document, 2004, available at: www.internetpolicy.net/governance/20040315paper.pdf;

779 For a brief history of the Internet, including its military origins, see: *Leiner, Cerf, Clark, Kahn, Kleinrock; Lynch, Postel, Roberts, Wolff*, A Brief History of the Internet, available at: www.isoc.org/internet/history/brief.shtml.

780 *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

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

782 For more information regarding anonymous communications, see below: § 3.2.I2.

783 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

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

785 See *Kahn/Lukasik*, Fighting Cyber Crime and Terrorism: The Role of Technology, presentation at the Stanford Conference, December 1999, page 6 *et seq.*; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 6, available at: http://media.hoover.org/documents/0817999825_1.pdf.

786 One example of the international cooperation of companies and delegation within international companies is the Compuserve case. The head of the German daughter company (Compuserve Germany) was prosecuted for making child pornography available that was accessible through the computer system of the mother company in the United States connected to the German company. See *Amtsgericht Muenchen*, Multimedia und Recht 1998, page 429 *et seq.* (with notes *Sieber*).

787 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

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

789 National Sovereignty is a fundamental principle in International Law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

790 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, page 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

791 See below: § 3.2.10.

792 See *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142.

793 Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA).

794 Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, page 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: http://.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

795 See: *Lewis*, Computer Espionage, Titan Rain and China, page 1, available at: www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf.

796 Regarding the extend of cross-border cases related to computer fraud, see: *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 9, available at: www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

797 See below: § 6.6.12.

798 See below: § 6.6.

799 One example is phishing. Although most sites are still stored in the United States (32%), which has strong legislation in place, countries such as China (13%), Russia (7%) and the Republic of Korea (6%), which may have less effective instruments in the field of international cooperation in place, are playing a more important role. Apart from the United States, none of them has yet signed and ratified cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

800 This issue was addressed by a number of international organizations. UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies". See below: § 5.1.

801 For more information, see http://en.wikipedia.org/wiki/ILOVEYOU. Regarding the effect of the worm on critical information infrastructure protection, see: *Brock*, ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000, available at: www.gao.gov/archive/2000/ai00181t.pdf.

802 BBC News, Police close in on Love Bug culprit, 06.05.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/738537.stm. Regarding the technology used, see: http://radsoft.net/news/roundups/luv/20000504,00.html.

803 See for example: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

804 One example of low-cost services that are automated is e-mail. The automation of registration allows providers to offer e-mail addresses free of charge. For more information on the difficulties of prosecuting cybercrime involving e-mail addresses, see: § 3.2.l2.

805 The term "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

806 For more details on the automation of spam mails and the challenges for law-enforcement agencies, see: *Berg*, The Changing Face of Cybercrime – New Internet Threats create Challenges to law enforcement agencies, Michigan Law Journal 2007, page 21, available at: www.michbar.org/journal/pdf/pdf4article1163.pdf.

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

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

809 Regarding the distribution of hacking tools, see: CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

810 See CC Cert, Overview of Attack Trends, 2002, page 1, available at: www.cert.org/archive/pdf/attack_trends.pdf.

811 Nearly 50 per cent of all fraud complains reported to the United States Federal Trade Commission are related to an amount paid between USD 0 and 25. See Consumer Fraud and Identity Theft Complain Data – January – December 2006, Federal Trade Commission, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

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

813 Gordon Moore observed that the power of computers per unit cost doubles every 24 months (Moore's Law).

814 Regarding the attacks, see: Lewis, Cyber Attacks Explained, 2007, available at: www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; A cyber-riot, The Economist, 10.05.2007, available at: http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007, available at: www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

815 See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

816 See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3, available at: www.cert.org/archive/pdf/Botnets.pdf.

817 See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, available at: www.cert.org/archive/pdf/Botnets.pdf; *Barford/Yegneswaran*, An Inside Look at Botnets, available at: http://pages.cs.wisc.edu/~pb/botnets_final.pdf; *Jones*, BotNets: Detection and Mitigation.

818 See Emerging Cybersecurity Issues Threaten Federal Information Systems, GAO, 2005, available at: www.gao.gov/new.items/d05231.pdf.

819 *Keizer*, Dutch Botnet Suspects Ran 1.5 Million Machines, TechWeb, 21.10.2005, available at: www.techweb.com/wire/172303160

820 See *Weber*, Criminals may overwhelm the web, BBC News, 25.01.2007, available at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/business/6298641.stm.

821 E.g. Botnets were used for the DoS attacks against computer systems in Estonia. See: *Toth*, Estonia under cyber attack, www.cert.hu/dmdocuments/Estonia_attack2.pdf.

822 "Over one million potential victims of botnet cyber crime", United States Department of Justice, 2007, available at: www.ic3.gov/media/initiatives/BotRoast.pdf.

823 *Staniford/Paxson/Weaver*, How to Own the Internet in Your Space Time, 2002, available at: www.icir.org/vern/papers/cdc-usenix-sec02/cdc.pdf.

824 *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International, 2006, page 142.

825 *Gercke*, Use of Traffic Data to trace Cybercrime offenders, DUD 2002, page 477 *et seq.*; *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

826 Regarding the necessary instruments, see below: § 6.5. One solution that is currently being discussed is data retention. Regarding the possibilities and risks of data retention, see: *Allitsch*, Data Retention on the Internet – A measure with one foot offside?, Computer Law Review International 2002, page 161 *et seq.*

827 The term “quick freeze” is used to describe the immediate preservation of data on request of law-enforcement agencies. For more information, see below: § 6.5.4.

828 The 24/7 network point pursuant to Art. 35 Convention on Cybercrime is a contact point appointed to reply to requests from law enforcement agencies outside the country. For more information, see below: § 6.6.8.

829 The graphical user interface called World Wide Web (WWW) was created in 1989.

830 The development of the graphical user interface supported content-related offences in particular. For more information, see above: § 2.6.

831 For more information see above: § 2.6.5.

832 Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

833 With regard to the interception of peer-to-peer based VoIP communications, law-enforcement agencies need to concentrate on carrying out the interception by involving the access provider.

834 Regarding the implications of the use of cell phones as storage media for computer forensics, see: *Al-Zarouni*, Mobile Handset Forensic Evidence: a challenge for Law Enforcement, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Al-Zarouni%20-%20Mobile%20Handset%20Forensic%20Evidence%20-%20a%20challenge%20for%20Law%20Enforcement.pdf.

835 On the advantages of wireless networks for the development of an IT infrastructure in developing countries, see: “The Wireless Internet Opportunity for Developing Countries”, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

836 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

837 Regarding the challenges related to anonymous communication, see: *Sobel*, The Process that “John Doe” is Due: Addressing the Legal Challenge to Internet Anonymity, Virginia Journal of Law and Technology, Symposium, Vol. 5, 2000, available at: www.vjolt.net/vol5/symposium/v5i1a3-Sobel.html.

838 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

839 Regarding legislative approaches requiring identification prior to the use of public terminals, see Art. 7 of the Italian Decree-Law No. 144. For more information, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.* and below: § 6.5.14.

840 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

841 Regarding the difficulties that are caused if offenders use open wireless networks, see above: § 3.2.3.

842 Regarding technical approaches in tracing back users of anonymous communication servers based on the TOR structure, see: *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

843 See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

844 Regarding the possibilities of tracing offenders using e-mail headers, see: *Al-Zarouni*, Tracing Email Headers, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Al-Zarouni.pdf.

845 *Donath*, Sociable Media, 2004, available at: http://smg.media.mit.edu/papers/Donath/SociableMedia.encyclopedia.pdf.

[846] Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Regarding the benefits of anonymous communication see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

[847] "(33) The introduction of itemised bills has improved the possibilities for the subscriber to check the accuracy of the fees charged by the service provider but, at the same time, it may jeopardise the privacy of the users of publicly available electronic communications services. Therefore, in order to preserve the privacy of the user, Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services [...]". Source: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[848] Article 37 – Traffic and billing data "1. Without prejudice to the provisions of paragraphs 2, 3 and 4, traffic data relating to users which are processed and stored to establish calls and other connections over the telecommunications network shall be erased or made anonymous upon termination of the call or other connection". – Regulation (EC) no 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

[849] See below: § 6.5.13.

[850] Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For further information on the Decree-Law, see, for example, the article "Privacy and data retention policies in selected countries", available at: www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

[851] Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[852] This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: "Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132.

[853] Regarding user-based approaches in the fight against cybercrime, see: *Goerling*, The Myth Of User Education, 2006 at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[854] The term "voice over Internet protocol" (VoIP) is use to describe the transmission technology for delivering voice communication using packet-switched networks and related protocols. For more information, see: *Swale*, Voice Over IP: Systems and Solutions, 2001; *Black*, Voice Over IP, 2001.

[855] Regarding the importance of interception and the technical solutions, see: *Karpagavinayagam/State/Festor*, Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection – ICIMP 2007. Regarding the challenges related to interception of data communication, see*: Swale/Chochliouros/Spiliopoulou/Chochliouros*, Measures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response, in *Janczewski/Colarik*, Cyber Warfare and Cyber Terrorism, 2007, page 424.

[856] Regarding the differences between PSTN and VoIP communication, see: *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq*.

[857] Regarding the interception of VoIP by law-enforcement agencies, see *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006; *Seedorf*, Lawful Interception in P2P-Based VoIP Systems, in *Schulzrinne/State/Niccolini*, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 *et seq*.

[858] Regarding the impact on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the mathematical background, see: *Menezes*, Handbook of Applied Cryptography, 1996, page 49 *et seq.*

859 74 per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: 2006 E-Crime Watch Survey, page 1, available at: www.cert.org/archive/pdf/ecrimesurvey06.pdf.

860 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

861 *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

862 *Kahn*, Cryptology goes Public, Foreign Affairs, 1979, Vol. 58, page 143.

863 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

864 Regarding the consequences for the law enforcement, Denning observed: "The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating". Excerpt from a presentation given by Denning, "The Future of Cryptography", to the joint Australian/OECD conference on Security, February, 1996. Regarding practical approaches to recover encrypted evidence see: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital
Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

865 Examples include the software Pretty Good Privacy (see http://www.pgp.com) or True Crypt (see www.truecrypt.org).

866 Regarding the use of cryptography by terrorists, see: *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf. *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

867 See: *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

868 *Denning/Baugh*, Encryption and Evolving Technologies as Tolls of Organised Crime and Terrorism, 1997, available at: www.cs.georgetown.edu/~denning/crypto/oc-rpt.txt.

869 Regarding the most popular tools, see: *Frichot*, An Analysis and Comparison of Clustered Password Crackers, 2004, page 3, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Frichot-1.pdf. Regarding practical approaches in responding to the challenge of encryption see: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf.

870 See: Data Encryption, Parliament Office for Science and Technology No. 270, UK, 2006, page 3, available at: www.parliament.uk/documents/upload/postpn270.pdf.

871 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

872 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

873 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

874 *Schneier*, Applied Cryptography, page 185; *Bellare/Rogaway*, Introduction to Modern Cryptography, 2005, page 36, available at: www.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

875 1 099 512 seconds.

876 *Usborne*, Has an old computer revealed that Reid toured world searching out new targets for al-Qaida?, The Independent, 18.01.2002, available at: http://www.independent.co.uk/news/world/americas/has-an-old-computer-revealed-that-reid-toured-world-searching-out-new-targets-for-alqaida-663609.html; *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf. With further reference to the case: *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

877 Equivalent to 10790283070806000000 years.

878 This technology is called BitLocker. For more information, see: "Windows Vista Security and Data Protection Improvements", 2005, available at: http://technet.microsoft.com/en-us/windowsvista/aa905073.aspx.

879 See *Leyden*, Vista encryption 'no threat' to computer forensics, The Register, 02.02.2007, available at: www.theregister.co.uk/2007/02/02/computer_forensics_vista/.

880 Regarding the encryption technology used by Skype (www.skype.com), see: *Berson*, Skype Security Evaluation, 2005, available at: www.skype.com/security/files/2005-031%20security%20evaluation.pdf.

881 Phil Zimmermann, the developer of the encryption software PGP, developed a plug-in for VoIP software that can be used to install added encryption, in addition to the encryption provided by the operator of the communication services. The difficulty arising from the use of additional encryption methods is the fact that, even if the law-enforcement agencies intercept the communications between two suspects, the additional encryption will hinder the analysis. For more information on the software, see: *Markoff*, "Voice Encryption may draw US Scrutiny", New York Times, 22.05.2006, available at: http://www.nytimes.com/2006/05/22/technology/22privacy.html?ex=1305950400&en=ee5ceb136748c9a1&ei=5088. Regarding the related challenges for law-enforcement agencies, see: *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

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

883 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; *Labs*, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

884 For practical detection approaches, see: *Jackson/Grunsch/Claypoole/Lamont*, Blind Steganography Detection Using a Computational Immune: A Work in Progress, International Journal of Digital Evidence, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04D31C4-A8D2-ADFD-E80423612B6AF885.pdf; *Farid*, Detecting Steganographic Messages in Digital Images, Technical Report TR2001-412, 2001; *Friedrich/Goljan*, Practical Steganalysis of Digital Images, Proceedings of SPIE Photonic West 2002: Electronic Imaging, Security and Watermarking of Multimedia Content IV, 4675, page 1 *et seq.*; *Johnson/Duric/Jajodia*, Information Hiding: Steganography and Watermarking, Attacks and Countermeasures, 2001.

885 See below: § 6.5.11.

886 See below: § 6.5.11.

887 See above: § 3.2.8.

888 See BBC News, Hacking: A history, 27.10.2000, available at: http://news.bbc.co.uk/1/hi/sci/tech/994700.stm.

889 An example of the integration of digital sources is Section 11, Subsection 3 of the German Penal Code: "Audio & visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection."

890 Within this process, the case-law based Anglo-American law system has advantages in terms of reaction time.

891 Computer Emergency Response Team. The CERT Coordination Center was founded in 1988 after the Morris worm incident, which brought 10 per cent of Internet systems to a halt in November 1988. For more information on the history of the CERT CC, see: www.cert.org/meet_cert/; *Goodman*, Why the Police don't Care about Computer Crime, Harvard Journal of Law and Technology, Vol. 10, Issue 3, page 475.

892 Examples of international cooperation in the fight against cybercrime include the Council of Europe Convention on Cybercrime and UN Resolution 55/63.

893 See below: § 5.

894 See above: § 2.8.1.

895 Regarding the offences recognized in relation to online games, see above: § 2.6.5.

896 Regarding the trade of child pornography in Second Life, see for example BBC, Second Life "child abuse" claim, 09.05.2007, at: http://news.bbc.co.uk/go/pr/fr/-/1/hi/technology/6638331.stm; Reuters, Virtual Child Pornography illegal in Italy, 23.02.2007, at: http://secondlife.reuters.com/stories/2007/02/23/virtual-child-porn-illegal-in-italy/.

897 *Gercke*, Zeitschrift fuer Urheber- und Medienrecht 2007, 289 *et seq.*

898 *Reuters*, UK panel urges real-life treatment for virtual cash, 14.05.2007, available at: http://secondlife.reuters.com/stories/2007/05/14/uk-panel-urges-real-life-treatment-for-virtual-cash/.

899 Regarding the use of ICTs by terrorist groups, see: *Conway*, Terrorist Use of the Internet and Fighting Back, Information and Security, 2006, page 16; *Hutchinson*, "Information terrorism: networked influence", 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/iwar/Hutchinson%20-%20Information%20terrorism_%20networked%20influence.pdf; *Gercke*, Cyberterrorism, Computer Law Review International 2007, page 64.

900 Data retention describes the collection of certain data (such as traffic data) through obliged institutions, e.g. access providers. For more details, see below: § 6.5.5.

901 Relating to these concerns, see: Advocate General Opinion, 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top.

902 *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

903 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

904 *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

905 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historic development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol.1, No.1.

906 *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

907 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq*.

908 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1.

909 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

910 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

911 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

912 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

913 Regarding the different models of cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also: *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

914 This includes the development of investigation strategies.

915 The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

916 See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

917 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

918 *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

919 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

920 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

921 This includes for example the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

922 This includes for example the identification of storage locations. See *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

923 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

924 *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

925 Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

4. 能力建设

参考书目（节选）： *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1; *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141*; Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf*; Henten/Samarajiva/ Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1; *Kellermann*, Technology risk checklist, Cybercrime and Security, IIB-2, page 1; *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003*; Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf; *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et seq.*; *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf.

公认的网络犯罪数量正在与日俱增，同时，即使在连接并不充分的发展中国家，受害者人数亦日渐增加，使得网络安全和网络犯罪成为私营部门和政府的热门议题。由于 ICT 发展如此迅速（在发展中国家尤其如此），建立和实施有效的反网络犯罪措施可谓十分重要。本章概要介绍了各国为应对频繁出现的问题而制定的此类应对措施。

4.1 网络安全和网络犯罪

在着手应对网络犯罪时，各国需首先需面对的一个问题是：开展此类工作应在执法环境还是网络安全环境中进行？对这两个问题加以区分是项颇具挑战性的工作。[926] 2010 年联合国大会有关网络安全的决议[927]将网络犯罪定性为一个主要挑战，这说明在上述两个问题之间存在着明确关联。因此，网络犯罪可被视为各类网络安全手段的组成部分[928]，不过，亦需承认，它只是网络安全战略的内容之一。虑及这一点不仅凸显了这两个问题的跨学科性质，同时亦说明，需要动员政府内部的利益攸关各方参与相关工作。在国家层面针对网络犯罪开展工作往往涉及不同部委（如司法部、交通部、教育部等）。

4.2 能力建设方法

我们对各国在打击网络犯罪时所需的不同能力建设方法进行了分析，分析结果表明，某些关键要素在最佳做法中可被视作基本要素。

4.2.1 规划

此类工作的起点是在国内（及与对口国际组织）进行有的放矢的讨论，以充分了解相关需求，并为起草一份相应的项目计划/建议做好准备。讨论过程将涵盖不同问题，例如：项目是否应包括战略和政策法规，还是仅将某些要素纳入其中？应起基础作用的现有结构是否已到位？在进行比较分析时，应以哪种国家、区域或国际标准为基准？应涵盖哪些问题（如保护上网儿童、数据保护、网络犯罪和电子交易）？项目是否还应涵盖专家培训和/或培训资料的开发等内容？国家是否正在获得其他支持？为在不同的支持活动间开展协调，了解不同活动的状态可谓极具现实意义。

4.2.2 制定项目规划

根据初步讨论结果，可制定一个项目规划草案，以对相关活动、参与专家、预期成果和时间表做出进一步描述。

4.2.3 以评估为起点

为启动项目，适当的评估是一个关键致胜因素。只有当所有参与官员和专家均了解了现有组件（如政策或立法）和细节（如一国有关法律起草的具体情况）后，才有可能为项目提供度身定制的支持。此类评估应涉及体制能力及对主要利益攸关方（如政府专家、企业协会和公民自由团体等兴趣小组）的确定。

4.2.4 对比分析

评估结果将说明现状如何，但不能具体描述一国相对于特定基准而言处于何种发展阶段。对比分析将在评估结果基础上进行，但可能会增加一个分析性组件。为进行对比，须首先确定相关基准，以明确可能存在的差距和突出最佳做法。若受益国为隶属于英联邦的一个太平洋小岛国，则可将现行国家立法或立法草案与英联邦有关计算机和计算机犯罪的示范法及支持太平洋岛屿国家的能力建设及信息通信技术政策、监管和立法框架（ICB4PAC）体系有关太平洋国家的区域模型框架进行对比。诸如有关信息系统攻击的欧盟指令或欧洲理事会《网络犯罪公约》等其他标准亦可被加至列表中。最终将形成一份复杂的报告，其中将对比或列出所确定的国家元素及基准中的可比元素，并指出两者的异同及提出建议。

4.2.5 与利益攸关方进行磋商

能力建设方法方面的另一个最佳做法是召集利益攸关方进行磋商。战略、政策和法律领域的多年能力建设经验表明，与利益攸关方进行磋商可大大推进起草过程。当然，为就国家政策和立法草案与广大利益攸关方进行讨论，大量工作的开展势在必行。不过，与国家利益攸关方进行磋商相当于经历了某种活学活用过程，此后的立法工作将因此得以顺利开展，这体现了在起草过程中进行深入讨论的价值所在，且可确保能够解决不同问题。

在国内进行此类磋商时，不同的国家利益攸关方（如普通公众、政治家、政府官员、产业界和商界、互联网服务提供商和公民自由团体）将受邀参加不同磋商会议，以就分析结果和拟议发展路径进行讨论。在起草政策和立法时，将注意到并纳入利益攸关方的相关输入意见。

4.2.5 起草过程

在对比分析和与利益攸关方进行磋商的基础上，可以制定或修订相关战略、政策和立法。起草过程通常还包括解释性说明和其他文件（如提交给内阁的简报文件）的起草工作。

4.2.6 培训、教育和跟进活动

最佳战略、政策和立法仍不足以有效地打击网络犯罪。其他措施（如专业人才的培养和对广大公众的教育）亦同样重要。为防范网络攻击，可行的培训活动包括针对特定年龄段学生的犯罪预防培训及针对政府高层官员的实时网络事件模拟等。后续活动通常还包括对此类项目的评估。

4.3 以战略为起点

正如之前所指出的那样，网络安全[929]在当前信息技术以及国际互联网服务的发展过程中起着重要作用。[930]加强国际互联网的安全性（以及保护国际互联网用户）已成为发展新业务以及政府政策的一个有机组成部分。[931]网络安全战略 — 例如，技术保护系统开发或者对用户进行教育，以防止成为网络犯罪的受害者 — 将有助于降低网络犯罪的风险。[932]

反网络犯罪战略应当成为网络安全战略的一个有机组成部分。国际电联的《全球网络安全议程》[933]是一个全球性的对话和国际合作框架，旨在协调国际社会应对日益严峻之网络安全挑战的响应行动，并增强对信息社会的信心和提高安全性，《议程》建立在现有的工作、倡议和合作关系基础之上，目标是提议制定一些全球战略，以应对这些相关的挑战。在《全球网络安全议程》五大支柱中所强调的所有必要措施，都与任何一种网络安全战略相关。此外，为了有效打击网络犯罪，要求在所有五大支柱中采取相关措施。[934]

4.3.1 现有战略的实施

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

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

采用现有反网络犯罪战略的发展中国家还需要考虑到其他几个问题，其中包括与相应法律体系的兼容性；支持倡议的状况（如社会的教育水平）；自我保护措施采用的程度；以及私营部门支持的程度（如通过公－私合作关系来支持）等。

4.3.2 区域差异

鉴于网络犯罪的国际特性，协调好各国的法律和技术，对打击网络犯罪而言至关重要。不过，协调工作必须考虑到不同的区域需求与能力。许多法律和技术标准得到了工业化国家的认可，但并未包含对发展中国家而言非常重要的各方面问题，这一事实突显了在实施反网络犯罪战略时考虑到区域方面问题的重要性。[935]因此，当在其他区域实施这些法律和技术标准时，需要考虑到区域因素和差异。

4.3.3 网络安全支柱内网络犯罪问题的关联性

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

4.3.4 战略的制定不仅局限于未来计划的制定

近年来，各国均制定了网络安全和网络犯罪战略。[936]国际组织和政府间机构亦概莫能外。在对不同方法加以比较后，便可发现在它们彼此之间存在太多相似之处。[937]

网络安全和网络犯罪战略多为篇幅短小的文件（10-20 页），且其中不会述及太多细节。战略多重点强调问题的现实意义、明确行动意愿及就改善网络安全应完成的任务做出总体决策。多数战略不会涉及具体解决方案和措施。战略的设计思路是就特定挑战或问题提供一种解决方案，且无需面面俱到，而只需就当前挑战提供指导意见。[938]例如，德国网络安全战略[939]便规定：政府应制定计划，以部署相关举措及检查提供商应承担的其他责任。不过，在相关工作的领导者及目标的达成方式方面，此类战略并未做出具体叙述。

基础性战略因制定时间短而独具优势。由于此类战略仅限于对一般性原则进行定义，因此无需定期更新。[940]较宏观战略在存在经年后进行更新都为时不晚。不过，此方法亦面临一些挑战。诚然，为确保所形成方法的全面性，固然不必将相关措施和活动归并到一份文件中。但是，若相关文件过于零散，则在不同措施之间或会无法互为观照。经验表明，在网络威胁的复杂性方面，在不同措施间即使存在小冲突或小矛盾亦可能大大降低事件防范和响应方法的有效性。只有当各类组件均保持统一且彼此呼应时，一种战略方可最大限度地发挥其效能。

为此，可采取以下折中方法，即：将宏观战略与作为后续行动的具体（亦因此更详细）行动计划合二为一。这种方法可向各方昭示为开展相关工作的确制定了网络犯罪和网络安全战略，但在具体措施方面又能做到秘而不宣。对各国政府而言，迫在眉睫的是需要针对网络犯罪和网络安全领域的活动进行概述，而制定国家网络安全战略对各国吸引投资方面亦可能存在重要意义。同时，为有针对性地打击罪犯，公开网络安全措施的细节未必会起到一劳永逸的效果，原因是攻击者亦可能因此获得用于识别网络漏洞的信息。

4.4 政策的现实意义

大多数国家甚少通过立法对此领域的某些行为定罪或提出调查手段。正常程序是首先出台一项政策。[941] 政策相当于一项战略，确定用于解决此问题的各种手段。更一般性的网络犯罪战略可能涉及利益攸关各方，而与此不同，政策的作用则是界定政府对某个问题做出的公开响应。[942] 这种响应不一定限于立法，因为政府有可用来实现政策目标的各种手段。即使所做决定认为有必要实施立法，也不一定需要单纯依靠刑法，亦可包括更侧重于预防犯罪的法规。在此方面，政府通过制定政策可全面界定其对某个问题做出的响应。鉴于打击网络犯罪的对策不能仅限于立法，还包括制定包含不同措施的各种战略，相关政策可以确保各项措施不会产生冲突。

在协调网络犯罪立法的各种方法中，对整合国家法律框架中的相关立法和将其纳入现有政策或首次制定此类政策的工作太不重视。因此，一些国家仅引入了网络犯罪立法，但政府并未制定反网络犯罪的战略及政策，因此遇到了严重的困难。出现这种情况的主要原因是缺乏预防犯罪的措施，且不同措施之间存在重叠。

4.4.1 政府内部职责

相关政策有助于政府内部对特定权能做出调整。不同部委之间职能的重叠现象并不稀奇 – 对于网络犯罪，由于它是一个跨学科的课题，这种现象经常发生。[943] 打击网络犯罪的相关问题可能涉及到司法部、通信部或国家安全部等多个部门的职责。各相关政府机构的职能可在制定有关政策的进程内加以界定。

例如，这在 ICB4PAC（支持太平洋岛屿国家的能力建设及信息通信技术政策、监管和立法框架）[944]《网络犯罪示范政策草案》（Draft Model Policy for Cybercrime）中有所阐述：

> 在此方面，必须明确规定利益攸关各方的责任。这一点尤其重要，原因是网络犯罪是一个跨部门的课题，可能涉及总检察长、通信部等不同机构的职责。

4.4.2 界定不同的组成部分

如上所述，政策可用来界定所采用的方法的不同组成部分，其中可包括从加强机构能力（如警力和监控）到具体的立法修订（如引入更先进的立法）等多方面的内容。

这是 ICB4PAC[945]《网络犯罪示范政策草案》中阐述的另一个问题：

> 要应对打击网络犯罪的多方面挑战，需要采用一种综合方法，其中应包括总体政策、立法、教育和提高认识、能力建设、研究以及技术方法。

理想的情况下，政策应用来协调各项活动（即使是不同部委和政府机构开展的活动）。政策通常需经内阁批准，因此不仅有助于确定相关课题涉及的各政府机构和部委，还有助于协调统一它们的活动。[946]

4.4.3 确定利益攸关方

政策不仅能确定相关的政府机构，还能确定应涉及的利益攸关方。如，可能有必要制定私营部门参与的指导方针。

例如，应涉及并解决的利益攸关方问题在 ICB4PAC[947]《网络犯罪示范政策草案》中有所阐述。

> 此外，这种方法需涉及政府、各部委和政府机构、私营部门、学校和大学、传统领袖、社区、国际和区域性机构、执法机构、法官、海关、检察官、律师、民间团体和非政府组织（NGO）等利益攸关各方。

4.4.4 确定基准

如下文进一步强调的那样，各区域性组织将统一立法的重要性确定为工作的重中之重。[948] 但需要统一的不仅限于立法 – 还包括战略和专家培训等问题。[949] 政策可用来确定应实现统一的领域以及界定应执行的区域和/或国际标准。

例如，统一的重要性在 ICB4PAC[950]《网络犯罪示范政策草案》中有所阐述：

> 鉴于网络犯罪的全球特性以及有必要防止本地区互联网用户成为网络犯罪的受害者，应作为优先事项，采取措施提高打击网络犯罪的能力。旨在应对网络犯罪挑战的战略和（特别是）立法一方面应符合国际标准，另一方面应反映本地区的独特性。

另一个示例是 HIPCAR《网络犯罪示范政策》[951]:

> 须就最常见的和国际广泛承认的网络犯罪形式以及本地区特别关注的那些罪行（如垃圾信息（SPAM））做出规定。
>
> 为了确保能与本地区内外各国的执法机关开展合作，立法须与国际标准和最佳做法以及（最大可能的程度上）与现有的区域标准和最佳做法保持一致。

4.4.5 确定立法的重点议题

政策可用来确定立法应涉及的重点领域。如，这可包括应涵盖的一系列罪行。详细程度可延伸至网络犯罪法律条文的细节。

HIPCAR《网络犯罪示范政策》是一个[952]:

> 其中应对蓄意和非法生产、销售儿童色情物品或相关行为定罪。尤其在此方面，应将国际标准纳入考虑范围。此外，立法还应对藏有儿童色情物品和访问儿童色情网站的行为定罪，并包括一项有助于执法机关开展调查的豁免规定。

4.4.6 确定需修正、更新或修改的法律框架

引入网络犯罪立法并非易事，因为需要监管的领域很多。除实体刑法和诉讼法外，网络犯罪立法可能还包括与国际合作、电子证据和互联网服务提供商（ISP）责任相关的问题。在大多数国家，这种立法的元素可能已经存在，但往往分散于不同的法律框架中。网络犯罪的相关规定并不一定需要在单项立法中实施。对于现有结构，可能有必要更新多项立法（如修正《证据法》，以确保对刑事诉讼中电子证据的可采性适用），或在引入新立法的进程内删除旧法（如《电信法》）条文。

这种沿用现有结构实施网络犯罪立法的做法肯定比在一项独立的法例中简单照搬区域标准或国际最佳做法更具挑战性。但鉴于这种从实际出发、量身定制的方法有利于保留本国的法律传统，许多国家倾向于这种做法。

政策可用来确定应整合的不同部分，以及需要更新的现有法律。

4.4.7 预防犯罪的重要性

虽然惩罚的威胁可能有预防犯罪的效应，但刑事立法的重点不是预防犯罪而是制裁犯罪。但预防犯罪被确定为有效打击网络犯罪的关键组成部分。[953] 相关措施可包括从技术解决方案（如防止非法入侵计算机系统的防火墙和可阻止安装恶意软件的防病毒软件）到限制访问非法内容等多个方面。[954]

例如，预防犯罪的重要性在 ICB4PAC [955]《网络犯罪示范政策草案》中有所阐述：

除了对网络犯罪定罪和提高执法能力来打击网络犯罪外，还需要制定预防犯罪的措施，其中包括从技术解决方案到提高用户认识等多方面的内容，在制定此类措施的过程中，有必要确定需特别关注的那些群体，如青年、对技术不太擅长的人（如来自技术闭塞的偏远村庄的人）和女性。但预防犯罪的措施亦应适用于更高端的用户和依赖于技术的参与者，如关键基础设施提供商（如旅游或金融业）。对必要措施的考虑应包括各种工具，如提高认识、提供和推广免费的防护技术（如防病毒软件）和实施能使家长限制某些内容的访问的解决方案。这些措施最好应在某项业务/技术引入时推出，并在其运作期间一直有效。为了扩大此类措施的适用范围，所涉及的利益攸关方应非常广泛，从互联网服务提供商到政府和区域性实体等，并探索各种资金来源。

4.5 监管机构在打击网络犯罪中的作用

在过去的几十年中，人们为解决网络犯罪问题讨论了各种方案，其中主要侧重于立法。但正如已在涉及反网络犯罪战略的章节中指出的那样，解决网络犯罪问题的综合方法的必要组成部分更为复杂。最近，焦点已集中在监管机构在打击网络犯罪中的作用上。

4.5.1 从电信监管到 ICT 监管

监管机构在电信领域的作用得到广泛的认可。[956] 由于互联网已消弱了政府与私营部门之间旧的职责分工模式，可看出 ICT 监管机构的传统角色和 ICT 监管重点已在发生转变。[957] 目前，ICT 监管机构已参与到与解决网络犯罪问题相关的一系列活动中。由于用户已变得脆弱，这对内容监管、网络安全和消费者保护等领域尤其重要。[958] 因此，监管机构的介入是网络犯罪破坏 ICT 产业及相关产品和服务发展的结果。

ICT 监管机构在打击网络犯罪中的新职责和新责任可看作从网络犯罪集中监管模式向灵活的结构转变的更广泛趋势的一部分。在一些国家，由于网络犯罪相关问题的出现，ICT 监管机构已研究了将监管职责的范围从电信行业内的竞争和授权问题转到更广泛的用户保护、产业发展、网络安全、参与网络犯罪的政策制定和实施上来，其中包括扩大 ICT 的应用范围。已设了一些新的监管机构负责包括网络犯罪在内的相关问题，[959] 而早已设立的 ICT 监管机构则已扩展其现有任务范围，将旨在解决网络相关威胁的各种活动包括进来。[960] 但这种干预的程序和限度仍在讨论中。

4.5.2 监管机构责任延伸模式

确定监管机构在打击网络犯罪方面的职责有两种模式，即扩充对现有职责范围的阐释，或确定新的职责。

监管机构进行干预的两个传统领域是消费者保护和网络安全。随着电信业务向互联网相关业务的过渡，消费者保护的重点发生了变化。除传统的威胁外，还需考虑到垃圾信息、恶意软件和僵尸网络的影响。荷兰独立邮电管理局（OPTA）就是职责延伸的例子。该监管机构的职责范围 [961] 包括禁止垃圾信息 [962] 和防范恶意软件的传播。[963] 在探讨 OPTA 的职责范围时，该组织表示应在作为传统活动领域的网络安全与网络犯罪之间建起一座桥梁，以有效解决这两个问题。[964] 如网络犯罪被视为网络安全管理的一种失利，那么监管机构的职责就因此自动得到扩展。

扩大监管机构的职责范围以纳入网络犯罪问题的可能性还取决于监管机构的机构设计，以及它是一个多部门监管机构（如公用事业委员会）、具体部门的电信监管机构还是一个融合的监管机构。从 ICT 行业监管的角度而言，每种机构设计模式都有其优缺点 [965]，在评估 ICT 监管机构应如何以及在何领域进行干预时应将机构设计类型纳入考虑范围。负责媒体和内容以及 ICT 业务的融合的

监管机构普遍在工作负荷的复杂性方面面临挑战。但它们包罗万象的职责在处理内容相关问题（如儿童色情物品或其他非法或有害内容）时却是一个优势。[966] 在融合的环境中，传统的电信监管机构可能在解决某些问题方面存在困难，如媒体内容和电信服务提供商之间的整合。融合的监管机构在解决内容-网络问题上似乎更有优势。此外，融合的监管机构能帮助避免监管的不一致和不确定性，以及在各种平台上传送的不同内容方面监管干预的不平衡性。[967]然而，对融合的监管机构的优势进行的讨论不应削弱单个部门监管机构所开展的活动的重要性。如截至 2009 年底，欧盟内只有四个融合的 ICT 监管机构，[968] 但参与解决网络犯罪问题的机构却远远多于这个数字。

在考虑扩充对现有职责范围的阐释时，必须考虑到监管机构的能力以及有必要避免与其他组织的职责范围产生重叠。如能对新的职责做出明确界定，则这种潜在的冲突就更容易得到解决。

第二种方法是确定新的职责。鉴于有产生冲突的可能性，马来西亚等国已决定对职责范围进行重新界定，以避免产生混淆和重叠。马来西亚通信与多媒体委员会（MCMC）是一个融合的监管机构，并已成立了一个专门的部门 [969] 来处理信息安全和网络可靠性、通信完整性和关键通信基础设施等问题。[970] 韩国采用了类似的做法，2008 年原信息通信部和韩国广播委员会合并成立了韩国通信委员会（KCC）。KCC 的其中一项职责是负责保护互联网用户免受有害或非法内容的影响。[971]

4.5.3 监管机构参与打击网络犯罪的示例

确定监管机构职责的模式以及 ICT 监管机构在此领域的行动范围都尚未得到明确界定。只有很少 ICT 监管机构有超越电信监管、处理更广泛的 ICT 部门问题的实际权力。处于这个日新月异、不断发展的部门，ICT 监管机构接触到历来被认为属于其他政府部门和机构职权范围或不属于任何部门权力范围的新领域。[972] 即使监管机构具有参与解决具体的网络犯罪相关问题的实际、充分的权能和行业专门知识，但针对确切干预领域的确定明确的职责范围是监管机构发挥作用的关键。下文重点对监管机构进行干预的潜在领域进行了阐述：

全球政策战略

国内分权原则[973]将政策制定和政策执行分离开来。[974] 尽管这一概念非常重要，但鉴于问题的复杂性，可能需要监管机构参与政策建议。[975] 由于具备行业专门知识，且已与其他利益攸关方建立起沟通渠道，许多国家的 ICT 监管机构在确定 ICT 行业发展的政策和战略方面发挥着重要的作用。[976] 因此在一些国家，向 ICT 政策制定进程提供意见被视为 ICT 监管机构的主要任务之一。[977] 虽然这一惯例侧重于针对电信问题提供意见和建议，但其职责范围可扩展到网络犯罪问题。芬兰政府成立了一个信息安全咨询委员会（ACIS），隶属于芬兰通信监管局（FICORA），来制定国家信息战略。[978] ACIS 在 2002 年发布的建议确定了提升信息安全战略的目标和措施。其中若干项措施可视为与网络犯罪问题相关，并强调了制定并完善适当立法、国际合作和提高最终用户信息安全认识的重要性。[979]

参与制定网络犯罪立法

通过立法的权能机构是立法机构，而非监管机构。但 ICT 监管机构可在制定网络犯罪立法的过程中发挥重要的作用。鉴于监管机构在数据保护、数据传输的保密性、防止恶意软件传播以及消费者保护和 ISP 责任等其他方面的经验，对监管机构在这些领域进行干预的讨论尤其热烈。[980] 此外，对监管机构而言，刑法不是一个未知的领域，因为在许多国家，严重违反传统监管工作领域义务的行为可能会受到刑事制裁。除上文强调的在整体战略方面的咨询作用外，监管机构还可参与立法起草进程。如乌干达通信委员会在立法起草过程中担任了顾问。[981] 此外，乌干达通信委员会通过乌干达国家网络犯罪立法任务小组参与了一项称为东非国家网络法任务组的区域性举措，该举措致力于持续发展和统一东非地区的网络犯罪法。[982] 据报道，赞比亚通信管理局 [983] 协助起草了新的网络犯

罪相关立法，[984] 即 2009 年《电子通信和交易法》。[985] 另一例子是比利时，2006 年比利时 ICT 监管机构（BIPT）在网络犯罪立法的起草过程中提供了协助。该草案是与英联邦法务部和英联邦计算机犯罪部合作制定的。[986]

网络犯罪侦查

计算机事件响应组（CIRT）在网络威胁和网络事件的监测、侦察、分析和调查方面发挥着重要的作用。[987] 由于网络犯罪问题的多部门特性，包括政府、企业、电信运营商和学术界在内的一系列利益攸关方建立了不同的 CIRT 来履行各种职能。[988] 在一些国家，ICT 监管机构负责国家 CIRT 的设立和管理。通常，这些 CIRT 不仅被视为国家层面负责侦查网络犯罪事件的主要实体，而且是增强国际层面网络犯罪合作的各种行动的主要参与者。首批作为 ICT 监管部门举措设立的 CIRT 包括 2002 年 1 月启动的芬兰国家计算机应急响应组，隶属芬兰通信监管局（FICORA）。[989] 其他还有瑞典、[990] 阿拉伯联合酋长国 [991] 和卡塔尔的例子。[992]

为执法提供便利

ICT 监管机构只能开展调查，并在此方面根据授予监管机构行使和执行具体法律条文的明确职责作为执法机构行事。一些国家授权 ICT 监管机构作为网络犯罪相关领域的执法机构，如反垃圾信息、内容监管或执行共同监管措施等。对于垃圾信息，欧洲一些 ICT 监管机构已加入欧洲理事会于 2004 年建立的反垃圾信息执法机关联络网，在泛欧洲层面打击垃圾信息。[993] OECD 垃圾信息任务组亦列出了作为执法机构联络方的 ICT 监管机构。[994] 在荷兰和罗马尼亚，ICT 监管机构与警方网络犯罪部门之间亦签署了合作协议。[995]

4.5.4 法律措施

在《全球网络完全协议》的五大支柱中，法律措施可能是与反网络犯罪战略最为相关的。

实体刑法

这首先需要制定必要的实体刑法条文，对计算机欺诈、非法访问、数据干扰、侵犯版权及儿童色情等行为定罪。[996] 虽然刑法中的一些规定对网络范围外的类似行为适用，但这不意味着这些规定对互联网上的行为同样适用。[997] 因此，对现行的国家法律进行分析是必要的，以查明可能存在的法律空白。[998]

诉讼法

除实体刑法外，[999] 执法机构还需要必要的工具和手段开展网络犯罪调查。[1000] 这种调查本身会带来一些挑战。[1001] 肇事者几乎可以从全世界任何地点实施犯罪行为，并采取措施掩饰其身份。[1002] 调查网络犯罪所需的工具和手段可能与普通犯罪行为的调查截然不同。[1003] 由于网络犯罪的国际性[1004]，还需制定能与国外执法机构实现合作的国家法律框架。[1005]

电子证据

有权能的调查机关以及法庭在处理网络犯罪时，需要涉及到电子证据。处理这类证据会带来一些挑战[1006]，但也为调查以及法医专家和法庭的工作提供新的可能性。[1007] 在没有其他证据来源的情况下，能否成功确定并起诉违法者可能取决于能否对电子证据进行妥善的收集和评估。[1008] 这会对执法机构和法庭处理这些证据方式产生影响。[1009] 传统证据是通过在法庭上提交原件进行介绍的，但在一些情况下数字证据需要特定的程序，而这些程序不允许将其转成传统证据（如凭文件和其他

所发现的资料的打印件）。[1010] 因此人们认为，证据可采性立法对打击网络犯罪而言是至关重要的。

国际合作

由于互联网的跨国性和业务的全球化，越来越多的网络犯罪呈现出了国际性。[1011] 希望与其他国际合作调查跨境犯罪的国家将需要诉诸国际合作的各种手段。[1012] 考虑到违法者的流动性，违法者是否在场与犯罪行为产生的影响之间并无关系，这提出了挑战，表明执法和司法机构有必要开展协作。[1013] 由于国家法律的差异且手段有限，国际合作被视为犯罪全球化的重要挑战之一。[1014] 在应对网络犯罪的综合方法中，各国有必要考虑加强与其他国家的合作能力，并提高这一程序的效率。

服务提供商的责任

如不借助互联网服务提供商（ISP）提供的服务，网络犯罪难以实施。包含威胁内容的电子邮件是通过电子邮件服务提供商提供的服务发送的，从某个网站下载非法内容则涉及托管服务提供商和接入服务提供商提供的服务。因此，在违法者利用 ISP 提供的服务作案的情况下，ISP 往往是刑事调查的关键。[1015] 鉴于一方面没有 ISP，网络犯罪不可能实施，另一方面提供商往往不具备防止这些犯罪行为的能力，这就提出了是否有必要限制互联网服务提供商责任的问题。[1016] 这一问题或许可在应对网络犯罪的综合法律方法内加以解决。

4.5.5 技术与程序措施

与网络犯罪有关的调查常常具有很强的技术性。[1017] 此外，要在调查期间维护证据的完整性，就需要严密的程序。因此，提升必需的能力以及制定必要的程序，是打击网络犯罪的一项必然要求。

另一个问题是开发技术保护系统。得到充分保护的计算机系统更难攻击。通过实施适当的安全标准来完善技术保护是重要的第一步。例如，修改网上银行系统（例如从 TAN [1018] 转为 ITAN [1019]），就大大消除了当前“网络钓鱼”攻击带来的风险，这充分展示了技术解决方案的至关重要性。[1020] 技术保护措施应包括技术基础设施的所有要素 — 核心网络基础设施以及世界范围内众多单独相连的计算机。为了保护互联网用户和企业，可以确定两个潜在的目标群：最终用户和企业（直接方法）；以及服务提供商和软件公司。

逻辑上，着重保护核心基础设施（如骨干网络、路由器、基本服务等），比起将数百万个用户融入到反网络犯罪战略中来要相对容易一些。对用户的保护可以通过确保消费者所用服务（如网上银行）的安全来间接实现。这种保护互联网用户的间接方法可以减少需纳入提升技术保护各环节的人员与机构数量。

尽管限制需纳入技术保护措施中的人员数量似乎是可取的，但计算机和国际互联网用户往往是网络安全中最薄弱的环节，是作案者的主要目标。相比攻击金融机构中受到充分保护的计算机系统，攻击个人计算机来获取敏感数据通常要容易一些。尽管存在这些逻辑问题，但保护好最终用户的基础设施对做好整个网络的技术保护而言是至关重要的。

互联网服务提供商和产品提供商（如软件公司）在支持反网络犯罪战略中起着非常重要的作用。由于他们直接与客户接触，因此他们可以扮演安全活动保证人的角色（例如，分发针对最新欺诈行为的保护工具和现状信息）。[1021]

组织结构

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

能力建设与用户教育

网络犯罪是一种全球现象。为了能够有效开展对违法行为的调查，需要协调各国的法律，并制定一些方法来开展国际合作。为了确保在发达国家和发展中国家中建立统一的全球标准，开展能力建设是必要的。[1022]

除了能力建设，还需要开展用户教育。[1023] 某些网络犯罪 — 特别是那些涉及欺诈的犯罪，如“网络钓鱼”和“电子欺骗”等 — 通常并非因为缺乏技术保护措施，而是因为受害者缺乏保护意识。[1024] 现有各种各样的软件产品可以自动识别伪冒的网站，[1025] 但到目前为止，这些产品无法识别所有可疑的网站。仅仅基于软件产品的用户保护战略大大限制了用户保护能力。[1026] 尽管技术保护措施仍在继续发展，而且可用的产品也在定期更新，但这些产品仍不能替代其他方法。

防止网络犯罪的最重要因素之一是用户教育。[1027] 例如，如果用户知道为其提供服务的金融机构绝不会通过电子邮件联系他们，要求其提供密码或银行账户的详细信息，那么他们就不会成为网络钓鱼或身份盗用攻击的受害者。对互联网用户的教育可减少潜在攻击目标的数量。对用户的教育可以通过以下方法进行：公共活动；学校、图书馆、信息技术中心和大学中的课程；公共－私人伙伴关系（PPP）。

对用户进行有效教育和制定信息战略的一项重要要求是公开最新的网络犯罪威胁。一些国家和/或私营企业为了避免客户对其在线通信服务失去信任，拒绝承认其公民与客户分别受到了网络犯罪威胁的影响。美国联邦调查局曾明确要求各公司克服其厌恶负面宣传的心理，如实报告网络犯罪威胁情况。[1028] 为了确定威胁等级，也为了告知用户，改进对相关信息的收集和公布是一项非常重要的工作。[1029]

国际合作

在许多情况下，互联网中的数据传送过程会影响一个以上的国家。[1030] 这是网络设计的必然结果，也是即使数据传送的直接线路临时受阻，协议也可确保传输能够成功进行的结果。[1031] 此外，大量的互联网服务（如托管服务等）是由国外的公司来提供的。[1032]

在这些情形中，违法者与受害者并非同处一个国家，而对网络犯罪调查来说，需要所有受影响国家的执法机构开展合作。[1033] 如果未获得相关国家主管部门的同意，是很难进行国际和跨国调查的，因为这涉及国家主权原则。这项原则一般不允许某个国家在未经当地主管部门许可的情况下在他国范围内进行调查。[1034] 因此，开展调查需要得到所有相关国家当局的支持。在大多数情况下，成功的网络犯罪调查只有一个很短的时间间隙，考虑到这一事实，当开展网络犯罪调查时，运用传统的相互法律援助体系就会面临一些明显的困难，原因是相互法律援助通常要求履行一些费时的正式程序。因此，进一步强化国际合作将在网络安全战略以及反网络犯罪战略的制定与实施中发挥重要而关键的作用。

4.6 非洲、加勒比和太平洋国家集团（非加太）的能力建设经验

自 2008 年至 2013 年，国际电联和欧盟共同资助了旨在推进非加太国家政策和立法工作的项目[1035]，此项目同时亦为“非加太信息通信技术”项目和第九届欧洲发展基金的组成部分。在撒哈拉以南的非洲地区，通过“非洲撒哈拉以南地区信息通信政策协调”项目（HIPSSA）提供了支持。

在加勒比国家实施了“通过 ICT 政策、立法和监管程序的协调来提高加勒比地区的竞争力”（HIPCAR）项目。[1036]在太平洋地区的国家，则通过支持太平洋岛屿国家的能力建设及信息通信技术政策、监管和立法框架（ICB4PAC）提供了支持。在这六年间，国际电联针对能力建设制定了具体方法，并取得了重要进展。

4.6.1 方法

上述项目的主要成就之一是在战略/政策/立法领域的能力建设综合方法方面取得了进展。为针对政策和法律问题进行区域协调，基于现有方法就最佳做法范例开展研究亦构成准备工作的一部分。但是，在所涉及的国家数目（涉及三个地区的逾 70 个国家）、工作领域（多达 9 个）和时间跨度（六年）方面，此项目均独树一帜，为此，探索新的工作方法便成为必然。

相关工作分为两个阶段，在第一阶段制定了区域示范政策和示范立法。在此阶段伊始，对受惠国的现有政策和立法进行了评估。为确保可囊括所有适用法律，评估工作由国际和区域专家领导，并得到了各国专门对口机构的支持。评估报告对调查结果进行了总结，并将现行标准与区域和国际最佳做法进行了对比，同时重点研究了至少可在一些受惠国直接适用的最佳做法（如英联邦示范法）。不过，评估报告中亦纳入了其他地区（如欧盟）的最佳做法。该报告[1037]还介绍了现行立法的概况，并对现行立法与区域和国际最佳做法做了对比分析。为就相关差距展开分析，评估报告还确定了国际最佳做法未必能够解决的特定区域需求。随后，所有受惠国的关键利益攸关方均就评估报告参与了讨论。在与利益攸关方进行磋商后，则针对各类相关工作领域推出了示范政策、示范法律和解释性说明。此工作由（所有受惠国的）区域专家领导，以确保可交付成果不仅与区域和国际最佳做法保持一致，实施起来亦能做到轻而易举。

第二阶段则在国家层面实现示范政策和示范立法的活学活用，为此需另行制定工作方法。因时间有限且工作领域众多，故需采取的工作方法应确保可在国内赢得有效支持。在明确了需开展的各项工作后，各国均获得了一个项目计划，此项目计划可确保针对各国特点提供专门支持。为确保各国的利益攸关方均能最大限度地提供支持，须在国家层面实现示范政策和示范立法的活学活用，为此则须与各类利益攸关方进行磋商。在磋商过程中，国家层面的各类利益攸关方（如：普通公众、政治家、政府官员、产业界和商界、互联网服务提供商和公民自由团体）均应邀参加了不同磋商会议，以就示范政策和示范立法及其活学活用问题进行公开讨论。起草过程涵盖并纳入了利益攸关方的输入意见。同时，地方和区域/国际专家则携手完成了起草工作。此外，还举办了面向不同利益集团的能力建设讲习班（如面向警察的专门培训；面向法官、地方治安官和检察官的单独会议、在学校和大学举办的讲座、面向普通公众的讲习班及与当地媒体携手开展的造势活动）。

4.6.2 所吸取的经验教训

与逾 70 个国家联手开展的大量工作衍生了不同最佳做法，这或许有助于未来的能力建设项目。

除立法外，政策亦不可或缺

为营造可靠的 ICT 使用环境，立法工作必不可少。[1038]但是，在战略和政策尚未出台之前，仅从立法层面启动相关工作并不常见。大多数国家均选择从出台政策入手。政策的作用是确定政府在某些问题上的立场[1039]，并帮助政府确定有关特定问题的总体基调。除立法外，这还可能涉及可用于实现政策目标的其他立场。与强调统一立法的其他区域性方法（如欧洲理事会《网络犯罪公约》[1040]）不同，HIPSSA、HIPCAR 和 ICB4PAC 亦涵盖了上述政策制定工作。其具体成果之一是简化了

与职能重叠的不同 ICT 利益攸关方（尤其是部委）的合作。利用政策和立法的组合拳亦可能会缩短在一国出台立法所需的时间。

示范法之间的有限差别

为应对具体犯罪（如非法访问），我们在不同区域性方法（如欧洲理事会《网络犯罪公约》[1041]、欧盟信息系统攻击框架决定[1042]、非洲联盟网络安全公约草案[1043]及 HIPSS、HIPCAR 和 ICB4PAC）之间进行了对比，结果表明：各区域在相关手段和方法的规定方面颇具异曲同工之处，且均遵循了国际最佳做法，因此，在加勒比专家制定的示范法基础上来开发 HIPSSA 和 ICB4PAC 示范框架便成为可能。

针对发展中国家的高标准

项目强调：小的发展中国家制定的标准未必要低于欧洲标准，事实上，此类国家的法律框架要素内容十分广泛，比欧洲标准有过之而无不及。儿童色情便是一例。在此方面，欧洲理事会《网络犯罪公约》第 9 条仅提及“描绘”儿童的“视觉资料”，音频资料则不属其中，但众所周知的是，在儿童色情问题上，犯罪分子亦会交换音频文件。[1044]HIPCAR、HIPSSA 和 ICBT 采用了与欧洲不同的表述方法，并避免了使用“视觉”一类术语，以将音频文件亦纳入其中。

专家广泛参与及与利益攸关方进行磋商的价值所在

在过渡阶段，有两项工作被证明价值卓然，即：几乎所有受惠国均派专家参与了示范政策和示范立法的起草工作，且国家利益攸关方在过渡阶段均广泛参与了相关工作。

对相关工作的评估表明，在制定区域标准的过程中，受惠国专家的广泛参与收获了丰硕果实。例如，在 47 个欧盟成员国中，仅有 14[1045]个成员国的专家及非成员国[1046]的四名专家参与了欧洲理事会《网络犯罪公约》的制定工作。与此不同的是，参与 HIPSSA、HIPCAR 和 ICB4PAC 示范政策和示范立法制定工作的专家几乎涵盖了所有受惠国。

另一个积极经验是召集利益攸关方进行了磋商。各方一致认为，与仅在内部进行讨论相比，与各利益攸关方就国家政策和立法草案的内容展开讨论需要投入大量精力。但是，利益攸关方的参与确保了随之的立法工作得以顺利开展，这表明了在起草过程中与各方推心置腹的价值所在，如此方可确保各方关注的问题均能得到解决。

926 Regarding a clear distinction see for example: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013), 1, page 3.

927 UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

928 See for example: ITU WTSA Resolution 50 (Rev. Johannesburg, 2008), on Cybersecurity, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.50-2008-PDF-E.pdf; ITU WTSA Resolution 52 (Rev. Johannesburg, 2008), on Countering and combating spam, available at: www.itu.int/dms_pub/itu-t/opb/res/T-RES-T.52-2008-PDF-E.pdf; ITU WTDC Resolution 45 (Doha, 2006), on Mechanism for enhancing cooperation on cybersecurity, including combating spam, available at: www.itu.int/ITU-D/cyb/cybersecurity/docs/WTDC06_resolution_45-e.pdf; European Union Communication: Towards a General Policy on the Fight Against Cyber Crime, 2007, available at: http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf; Cyber Security: A Crisis of Prioritization,

President's Information Technology Advisory Committee, 2005, available at: www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

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

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

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

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

933 For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

934 See below: § 4.4.

935 The negotiations regarding the Convention on Cybercrime took place not only between members of the Council of Europe. Four non-members (the United States, Canada, South Africa and Japan) were involved in the negotiations, but no representatives of countries from the African or Arab regions.

936 See for example: Austria: National ICT Security Strategy Austria, available at: www.ccdcoe.org/strategies/Austrian_Cyber_Security_Strategy.pdf; Estonia: Cyber Security Strategy, available at: www.kaitseministeerium.ee/files/kmin/img/files/Kuberjulgeoleku_strateegia_2008-2013_ENG.pdf; Germany: Cybersecurity Strategy for Germany, available at: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile; United Kingdom: UK Cyber Security Strategy, available at.: www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf; New Zealand: www.dpmc.govt.nz/sites/all/files/publications/nz-cyber-security-strategy-june-2011_0.pdf; For more examples see: National Cyber Security Framework Manual, NATO CCD, 2012, page 53 et seq.

937 See for example the EU Cybersecurity Strategy: Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN (2013), 1. Regarding the activities of the UN in relation to Cybersecurity see: Maurer, Cyber Norm Emergence at the United Nations, An Analysis of the Activities at the UN regarding Cyber-Security, 2011.

938 See: National Cyber Security Framework Manual, NATO CCD, 2012, page 46.

939 Cybersecurity Strategy for Germany, 2011, page 7, available at: www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

940 With regard to the need of updates see below III.5.c..

941 This issue was for example taken into consideration within the EU/ITU co-funded projects HIPCAR and ICB4PAC. The model policy, as well as the model legislation, are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

942 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

943 Regarding the need for an interdisciplinary approach see: *Schjolberg/Ghernaouti-Helie*, A Global Treaty on Cybersecurity and Cybercrime, Second Edition, 2011, page 17, available at: www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf.

944 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

945 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

946 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

947 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

948 See below: § 5.

949 The harmonization of training is one of the main objectives for the EU Cybercrime Centers of Excellence Network (2Centre). Information is available at: www.2centre.eu. Other examples are the European Cybercrime Training & Education Group (ECTEG) as well as the Europol Working Group on the Harmonization of Cybercrime Training (EWGHCT).

950 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

951 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

952 The text is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/reports/wg2/docs/HIPCAR_1-5-B_Model_Policy_Guidelines_and_Legislative_Texts_Cybercrime.pdf.

953 See for example: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, 2007, page 5, available at: www.penal.org/IMG/Guadalajara-Vogel.pdf; *Pladna*, The Lack of Attention in the Prevention of Cyber Crime and How to improve it, University of East Carolina, ICTN6883, available at: www.infosecwriters.com/text_resources/pdf/BPladna_Cybercrime.pdf.

954 Regarding blocking of websites with illegal content see: *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008.

955 The approved documents related to the projects are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

956 Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary, page 7, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf; see also ITU, World Summit on Information Society, The Report of the Task Force on Financial Mechanisms for ICT for Development, December, 2004, available at: www.itu.int/wsis/tffm/final-report.pdf; ITU/infoDEV ICT Regulation Toolkit, Chapter 4.1. What is the Role of Regulators?, available at: www.ictregulationtoolkit.org/en/Section.3109.html

957 See GSR09 – Best Practice Guidelines on innovative regulatory approaches in a converged world to strengthen the foundation of a global information society, available at www.itu.int; *Macmillian.* Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009 // available at: http://www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf

958 *Stevens*, Consumer Protection: Meeting the expectation of connected Consumer. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Consumer-protection_Stevens.pdf; *Macmillian*, Connectivity, Openness and Vulnerability: Challenges Facing Regulators. GSR Discussion Paper 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR09_Challenges-regulators_Macmillan.pdf.

959 E.g. Korea Communications Commission, established in February 2008 (formed after consolidating the former Ministry of Information and Communication and the Korean Broadcasting Commission), announced among other core regulatory duties protection of Internet users from harmful or illegal content. Korea Communications Commission: http://eng.kcc.go.kr.

960 E.g. Swedish ICT Regulator PTS addresses cyberthreats and cybercrime under user protection mandate and network security mandate. See: *PTS*. Secure communications, available at www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

961 *OPTA*. Regulatory areas, available at: www.opta.nl/en/about-opta/regulatory-areas/.

962 The Dutch regulator is granted the mandate to monitor any contravention of the prohibition of unsolicited communication under its duties to provide Internet safety for consumers.

963 OPTA has the power to take action against anyone contravening the prohibition of spam and unsolicited software by imposing fines.

964 OPTA Reaction on the Consultation Concerning the Future of ENISA, 14/01/2009, available at: http://ec.europa.eu/information_society/policy/nis/docs/pub_consult_nis_2009/public_bodies/OPTA.pdf.

965 *Spyrelli*, Regulating The Regulators? An Assessment of Institutional Structures and Procedural Rules of National Regulatory Authorities, International Journal of Communications Law and Policy, Issue. 8, Winter. 2003/2004; *Henten/ Samarajiva/ Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; infoDev/ITU ICT regulation Toolkit, available at: www.ictregulationtoolkit.org/en/Section.2033.html.

966 See the discussions on regulation, illegal content and converged regulators: *Van Oranje et al,* Responding to Convergence: Different approaches for Telecommunication regulators TR-700-OPTA, 30 September 2008, available at: www.opta.nl/download/convergence/convergence-rand.pdf; *Millwood Hargrave, et al,* Issues facing broadcast content regulation, Broadcasting Standards Authority, New Zealand, 2006, available at: www.bsa.govt.nz/publications/IssuesBroadcastContent-2.pdf. See also: *ITU*, Case Study: Broadband, the Case of Malaysia, Document 6, April 2001, available at: www.itu.int/osg/spu/ni/broadband/workshop/malaysiafinal.pdf.

967 See*: infoDev/ITU* ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html. See also: *Henten/ Samarajiva/Melody,* Designing next generation telecom regulation: ICT convergence or multi-sector utility?, info, 2003, Vol. 5 Issue 1, page 26-33; *Singh/Raja*, Convergence in ICT services: Emerging regulatory responses to multiple play, June 2008, available at: http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/Convergence_in_ICT_services_Emerging_regulatory_responses_to_multiple_play.pdf; *Garcia-Murillo*, Regulatory responses to convergence: experiences from four countries, Info, 2005, Volume 7, Issue 1.

968 The four states which have regulators that can be regarded as converged regulatory authorities are: Finland, Italy, Slovenia and the United Kingdom. See: infoDev/ITU ICT Regulation Toolkit, Chapter 2.5. Convergence and Regulators, available at: www.ictregulationtoolkit.org/en/section.3110.html.

969 Information and network security (INS).

970 See: *MCMC*, What do we Do. Information Network Security, available at: www.skmm.gov.my/what_we_do/ins/feb_06.asp.

971 Korea Communications Commission: Important Issues, available at: http://eng.kcc.go.kr.

972 Trends in Telecommunication Reform 2009. Hands-On or Hands-Off? Stimulating Industry Growth through Effective ICT Regulation. Summary. 2009, P. 11, available at: www.itu.int/dms_pub/itu-d/opb/reg/D-REG-TTR.11-2009-SUM-PDF-E.pdf.

973 See: *Haggard/McCubbins*, Presidents, Parliaments, and Policy. University of California, San Diego, July 1999, available at: http://mmccubbins.ucsd.edu/ppp.pdf. For the discussion with regard to regulatory agencies, see: *Maggetti*, The Role of Independent Regulatory Agencies in Policy-Making: a Comparative Analysis of Six Decision-Making Processes in the Netherlands, Sweden and Switzerland. IEPI, University of Lausanne, available at: http://regulation.upf.edu/ecpr-07-papers/mmaggetti.pdf.

974 The rationale for separating the ICT regulator from the policy-making body is to have an independent regulator that maintains a distance from the ministry or other government bodies which could remain as the major shareholder of the incumbent. An independent regulator can avoid conflict of interest that can happen if the regulator is also responsible for industry promotion. See: *OECD*, Telecommunications Regulatory Structures and Responsibilities, DSTI/ICCP/TISP(2005)6/FINAL, January, 2006, available at: www.oecd.org/dataoecd/56/11/35954786.pdf.

975 InfoDev ITU ICT Regulation toolkit. Section 6.3. Separation of Power and Relationship of Regulator with Other Entities, available at: www.ictregulationtoolkit.org/en/Section.1269.html.

976 Public Consultation Processes. InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/En/PracticeNote.756.html; *Labelle*, ICT Policy Formulation and e-strategy development, 2005, available at: www.apdip.net/publications/ict4d/ict4dlabelle.pdf.

977 One example is the Botswana Telecommunications Authority, which is required to provide the input to government policy-making efforts. See: Case Study Single Sector Regulator: Botswana Telecommunications Authority (BTA). InfoDev ITU ICT Regulation Toolkit, available at: www.ictregulationtoolkit.org/en/PracticeNote.2031.html.

978 International CIIP Handbook 2008/2009, Center for Security Studies, ETH, Zurich, 2009, available at www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663, P. 133.

979 National Information Security Strategy Proposal, November, 2002 // available at: www.mintc.fi/fileserver/national_information_security_strategy_proposal.pdf.

980 *Lie / Macmilian*, Cybersecurity: the Role and Responsibilities of an Effective Regulator. Draft Background Paper. 9th ITU Global Symposium for Regulators. 2009, available at: www.itu.int/ITU-D/treg/Events/Seminars/GSR/GSR09/doc/GSR-background-paper-on-cybersecurity-2009.pdf.

981 See: *Uganda Communications Commission*, Recommendations on Proposed Review of the Telecommunications Sector Policy, 2005, available at: www.ucc.co.ug/UgTelecomsSectorPolicyReview_31_Jan_2005.pdf; *Blythe*, The Proposed Computer Laws of Uganda: Moving Toward Secure E-Commerce Transactions and Cyber-Crime Control in Repositioning African Business and Development for the 21st Century, Simon Sigué (Ed.), 2009, available at: www.iaabd.org/2009_iaabd_proceedings/track16b.pdf; Uganda Computer Misuse Bill 2004, available at: www.sipilawuganda.com/files/computer%20misuse%20bill.pdf.

982 See, for example: Report of the Second EAC Regional Taskforce Meeting on Cyber Laws. June 2008, Kampala, Uganda, available at: http://r0.unctad.org/ecommerce/event_docs/kampala_eac_2008_report.pdf.

983 Now: Zambia Information and Communications Technology Authority.

984 *Mukelabai*, Cybersecurity Efforts in Zambia. Presentation at ITU Regional Cybersecurity Forum for Africa and Arab States 4th – 5th June 2009 Tunis, Tunisia, available at: www.itu.int/ITU-D/cyb/events/2008/lusaka/docs/mukelabai-caz-zambia-lusaka-aug-08.pdf; *Hatyoka*, ZICTA Corner – Defining ZICTA's new mandate. Times of Zambia, 2009 // available at: www.times.co.zm/news/viewnews.cgi?category=12&id=1262768483.

985 Zambia Electronic Communications and Transactions Act 2009, available at: www.caz.zm/index.php?option=com_docman&Itemid=75. See also ZICTA. Cybercrime Penalties (Part 1), available at: www.caz.zm/index.php?option=com_content&view=article&id=76:cyber-crime-penalties-part-1&catid=34:column&Itemid=38.

986 Annual report 2008 Belgian Institute for postal service and telecommunication, BIPT, 2009, available at: http://bipt.be/GetDocument.aspx?forObjectID=3091&lang=en.

987 See: *Killcrece, et al,* Organizational Models for Computer Security Incident Response Teams (CSIRTs). Handbook, December, 2003, available at: www.cert.org/archive/pdf/03hb001.pdf.

988 *Scarfone/Grance/Masone,* Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology. NIST Special Publication 800-61, 2008, available at: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf, pp. 2-2.

989 www.ficora.fi/.

990 Sweden's IT Incident Centre (Sitic) is located in the ICT regulator PTS .See: PTS. Secure communications, available at: www.pts.se/en-gb/About-PTS/Operations/Secure%20communications/.

991 aeCERT created as an initiative of the UAE Telecommunications Regulatory Authority to detect, prevent and respond to current and future cybersecurity incidents in the UAE *: Bazargan*, A National Cybersecurity Strategy aeCERT Roadmap. Presentation at Regional Workshop on Frameworks for Cybersecurity and CIIP 18 – 21 Feb 2008 Doha, Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/doha/docs/bazargan-national-strategy-aeCERT-doha-feb-08.pdf.

992 The national CERT (qCERT) was established by the Qatari ICT regulator (ictQatar) and acts on behalf of ictQatar; *Lewis*, Q-CERT. National Cybersecurity Strategy Qatar, available at: www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incid ent-management-brisbane-july-08.pdf.

993 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf.

994 E.g. ICT regulators are involved in law-enforcement efforts with regard to combating spam in the following countries: Australia, Finland, Greece, Hungary, Japan, Malaysia, Mexico, Netherlands, Portugal, Turkey. See: *OECD* Task Force on Spam. Enforcement authorities contact list, available at: www.oecd-antispam.org/countrycontacts.php3.

995 *Time.lex.* Study on activities undertaken to address threats that undermine confidence in the information society, such as spam, spyware and malicious software. SMART 2008/ 0013, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/ext_studies/privacy_trust_policies/spam_spyware_legal_study2009final.pdf. Page 21.

996 *Gercke*, The Slow Wake of a Global Approach Against Cybercrime, Computer Law Review International 2006, page 141. For an overview of the most important substantive criminal law provisions, see below: § 6.2.

997 See *Sieber*, Cybercrime, The Problem behind the term, DSWR 1974, page 245 *et. seq*.

998 For an overview of cybercrime-related legislation and its compliance with the standards defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/. See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

999 See below: § 6.2.

1000 See below: § 6.2.

1001 For an overview of the most relevant challenges in the fight against cybercrime, see above: § 3.1.

1002 One possibility to mask identity is the use of anonymous communication services. See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999. Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf. Regarding anonymous file-sharing systems, see: *Clarke/Sandberg/Wiley/Hong*, Freenet: a distributed anonymous information storage and retrieval system, 2001; *Chothia/Chatzikokolakis*, A Survey of Anonymous Peer-to-Peer File-Sharing, available at: www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf; *Han/Liu/Xiao/Xiao*, A Mutual Anonymous Peer-to-Peer Protocol Desing, 2005.

1003 Regarding legal responses to the challenges of anonymous communication, see below: §§ 6.5.10 and 6.3.11.

1004 See above: § 3.2.6.

1005 See in this context below: § 6.6.

1006 *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

1007 *Vaciago*, Digital Evidence, 2012.

1008 Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

1009 Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

1010 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

1011 Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1012 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[1013] See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[1014] *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

[1015] See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

[1016] For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[1017] *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

[1018] Transaction authentication number – for more information, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

[1019] The ITAN system improves the TAN system. The financial institutions provide the customer with a number of TAN-indexed identity numbers. With regard to each relevant transaction, the online banking system requires a specific ITAN number selected at random from the list of supplied TAN. For more information, see: *Bishop*, Phishing & Pharming: An investigation into online identity theft, 2005, available at: http://richardbishop.net/Final_Handin.pdf.

[1020] Regarding various authentication approaches in Internet banking, see: Authentication in an Internet Banking Environment, United States Federal Financial Institutions Examination Council, available at: www.ffiec.gov/pdf/authentication_guidance.pdf.

[1021] Regarding approaches to coordinate the cooperation of law-enforcement agencies and Internet service providers in the fight against cybercrime, see the results of the working group established by Council of Europe in 2007. For more information, see: www.coe.int/cybercrime/.

[1022] Capacity building is in general defined as the creation of an enabling environment with appropriate policy and legal frameworks, institutional development, including community participation (of women in particular), human resources development and strengthening of managerial systems. In addition, UNDP recognizes that capacity building is a long-term, continuing process, in which all stakeholders participate (ministries, local authorities, non-governmental organizations, user groups, professional associations, academics and others).

[1023] At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect". Regarding user-education approaches in the fight against phishing, see: Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, Technical Trends in Phishing Attacks, available at: www.cert.org/archive/pdf/Phishing_trends.pdf. Regarding sceptical views on user education, see: *Görling*, The Myth Of User Education, 2006, available at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

[1024] Anti-Phishing Best Practices for ISPs and Mailbox Providers, 2006, page 6, available at: www.anti-phishing.com/reports/bestpracticesforisps.pdf; *Milletary*, "Technical Trends in Phishing Attacks", available at: www.cert.org/archive/pdf/Phishing_trends.pdf.

[1025] *Shaw*, Details of anti-phishing detection technology revealed in Microsoft Patent application, 2007, available at: http://blogs.zdnet.com/ip-telephony/?p=2199; Microsoft Enhances Phishing Protection for Windows, MSN and Microsoft Windows Live Customers – Cyota Inc., Internet Identity and MarkMonitor to provide phishing Web site data

for Microsoft Phishing Filter and SmartScreen Technology services, 2005, available at: www.microsoft.com/presspass/press/2005/nov05/11-17EnhancesPhishingProtectionPR.mspx.

1026 For a different opinion, see: *Görling*, The Myth Of User Education, 2006, at: www.parasite-economy.com/texts/StefanGorlingVB2006.pdf.

1027 At the G8 Conference in Paris in 2000, *Jean-Pierre Chevenement*, the French Minister of Interior, stated: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

1028 "The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful hacker attack, explained Mark Mershon, acting head of the FBI's New York office." See Heise News, 27.10.2007, available at: www.heise-security.co.uk/news/80152.

1029 Examples of the publication of cybercrime-related data include: Symantec Government Internet Security Threat Report Trends for July–December 06, 2007, available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf; Phishing Activity Trends, Report for the Month of April 2007, available at: www.antiphishing.org/reports/apwg_report_april_2007.pdf.

1030 Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1031 The first defined and still most important communication protocols are: TCP (Transmission Control Protocol) and IP (Internet Protocol). For further information, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

1032 See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding the possibilities of network-storage services, see: *Clark*, Storage Virtualisation Technologies for Simplifying Data Storage and Management.

1033 Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cyber Crime, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 35 *et seq.*, available at: http://media.hoover.org/documents/0817999825_35.pdf; Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

1034 National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

1035 Details about the project and the funding are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/

1036 For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html; ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 4.

1037 The assessment reports are available on the HIPCAR website and will be on the HIPSSA and ICB4PAC website shortly.

1038 With regard to the relevance of legislation related to the specific topic cybercrime see: Gercke, CRi 2012, 81.

1039 See for example: The Queensland Legislation Handbook, 2004, Chapter 2.2, available at: www.legislation.qld.gov.au/Leg_Info/publications/Legislation_Handbook.pdf.

1040 Council of Europe Convention on Cybercrime (CETS No. 185); *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225,; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, CRi 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, CRi 2008, page 7 *et seq.*; *Gercke*, 10 years Convention on Cybercrime, Cri 2011, 142 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

1041 Art. 2: Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

[1042] Art. 2 (1) :Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases which are not minor.

[1043] Art. III-2: Each Member State of the African Union shall take the legislative measures required to set up as a penal offense the fact of accessing or attempting to access fraudulently a part or the whole of a computer system.

[1044] Regarding the relevance of audio files see: *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1045] Belgium, Bulgaria, Czech Republic, Estonia, Finland, France, Germany, Greece, Italy, Latvia, Netherlands, Portugal, Sweden and "The Former Yugoslav Republic of Macedonia".

[1046] The decision to establish the working group was made during the 583rd Meeting of the Minister's, Decision No. CM/Del/Dec(97)583.

5. 区域性组织和国际组织活动概述

参考书目（节选）： *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009; Committee II Report, 11th UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007; *Nilsson* in *Sieber*, Information Technology Crime, page 576; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001; Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, 2001; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07.

本章将简要介绍国际法律方法[1047]及其与国家层面的立法途径的关系。

5.1 国际方法

许多国际组织一直致力于分析网络犯罪的最新进展，并建立了一些工作小组，负责制定打击网络犯罪战略。

5.1.1 七国集团（之前为八国集团）[1048]

1997 年，八国集团（G8）成立了“高科技犯罪分委员会[1049]”，负责打击网络犯罪。[1050] 八国集团的司法与内政部长在美国华盛顿特区举行峰会期间通过了打击高科技犯罪的《十项原则》和《十点行动计划》。[1051] 随后，八国首脑签署了这些原则，其中包括：

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

1999 年，在俄罗斯联邦首都莫斯科召开的打击跨国有组织犯罪部长级会议上，八国集团确定了打击高科技犯罪的具体规划。[1052] 它们表达了对跨国有组织犯罪（例如儿童色情）、交易的可追溯性以及越境访问存储数据等问题的关注。会议公报中包含了诸多打击网络犯罪的原则，这些原则已成为许多国际战略的基础和依据。[1053]

专家组已经取得的实际工作成果之一是提出建立 24/7一国际联络网络，要求各参与国为跨国调查建立联络点，联络点每周 7 天、每天 24 小议都处于运行状态。[1054]

2000 年，在法国巴黎的八国集团大会上，八国集团提出了网络犯罪的议题，并呼吁各国杜绝非法的数字避风港。当时，八国集团已经将其寻求国际解决方案的努力与欧洲理事会的《网络犯罪公约》结合起来。[1055] 2001 年，在日本东京举行的研讨会上，[1056] 八国集团讨论了打击网络犯罪的程序手段，焦点在于是应当履行数据保留义务，还是将数据保留作为一种替代解决方案。[1057]

2004 年，八国集团司法和内政部长会议发表了一份公报，在公报中提出了在打击使用国际互联网的犯罪活动时，需要全球范围内的能力建设。[1058] 八国集团再次提到了欧洲理事会《网络犯罪公约》。[1059]

在 2006 年莫斯科会议期间，八国集团司法和内政部长们讨论了与打击网络犯罪相关的问题以及网络空间问题，并特别提到需要改进有效的措施。[1060] 八国集团司法和内政部长会议之后召开了八国集团莫斯科峰会，会议讨论了有关网络恐怖主义 [1061] 的议题。[1062]

2007 年，在德国慕尼黑举行的八国集团司法和内政部长会议进一步讨论了恐怖分子使用国际互联网的问题，与会各国同意对恐怖组织滥用国际互联网的行为予以定罪。[1063] 该协议未涵盖各国应予定罪的某些特定行为。

2009 年，在意大利罗马举行的八国集团司法和内政部长会议对有关网络犯罪的若干问题进行了讨论。会议的最终宣言表示，八国集团认为应根据国际组织更新和分发的黑名单封锁儿童色情网站。[1064] 就网络犯罪总体情况而言，最终宣言强调，网络犯罪已经成为日益严重的威胁，宣言指出有必要增进服务提供商和执法机构之间的合作，并需要强化现有合作形式，例如 G8 24/7 高科技犯罪联络点。[1065]

在加拿大马斯科卡举行的八国集团峰会仅简要讨论了网络犯罪问题。《马斯科卡宣言》仅在涉及恐怖分子活动的内容中提到，八国集团对网络犯罪日益严重的威胁深表关切，并将通过进一步的努力削弱恐怖分子和犯罪组织的势力。[1066]

八国集团电子论坛（在此论坛中，代表团和企业界领导人就互联网相关主题展开讨论 [1067]）和在法国多维尔召开的八国集团峰会都对网络犯罪和网络安全问题展开了讨论。然而，尽管此次峰会的最终宣言亦如往届会议一样，对网络犯罪这一主题给予了较高关注，但宣言并未提出任何具体建议。八国集团仅对部分一般性原则（如安全问题和防止犯罪行为对于巩固发展繁荣强大的互联网的重要性等）达成了共识。[1068]

5.1.2 联合国及联合国毒品和犯罪问题办事处[1069]

为应对网络犯罪带来的挑战，联合国已经采取了若干重要措施。这些措施已经从最初的仅限于制定概括性的指导原则，发展成为目前更加深入地应对挑战并采取法律对策。

《联合国儿童权利公约》

《联合国儿童权利公约》于 1998 年得到通过，[1070] 其中包含多份旨在保护儿童的法律文书。公约并未对儿童色情做出定义，亦未包含有关将传播网上儿童色情内容的行为定罪的条款。然而，公约第 34 条呼吁各成员国采取一切措施防止利用儿童从事色情表演。

联合国大会第 45/121 号决议

在第八届联合国预防犯罪和罪犯待遇大会（于 1990 年 8 月 27 日-9 月 7 日在古巴哈瓦那召开）之后，联合国大会通过了一项有关计算机犯罪立法的决议。[1071] 根据第 45/121 号决议（1990 年），联合国在 1994 年出版了一本有关预防和控制计算机相关犯罪的手册。[1072]

《儿童权利公约关于买卖儿童、儿童卖淫和儿童色情制品问题的任择议定书》

该任择议定书不仅涉及一般性的儿童色情制品问题，还明确指出了互联网在散布此类资料过程中的作用。[1073] 儿童色情制品是指以任何手段展示儿童进行真实或模拟的直露性活动或者主要以性目的展示儿童性器官的制品。[1074] 议定书第 3 条要求各缔约方将某些行为 – 包括与儿童色情制品相关的行为 – 定为犯罪行为。

> ***第 3 条***
>
> *1* 每一缔约国应起码确保本国刑法对下列行为和活动作出充分的规定,不论这些犯罪行为是在国内还是跨国实施的,也不论是个人还是有组织地实施的:
>
> [...]
>
> *(c)* 为上述目的制作、分销、传送、进口、出口、出售、销售或拥有第 2 条所界定的儿童色情制品。
>
> [...]

第十届联合国预防犯罪和罪犯待遇大会

于 2000 年在维也纳召开的第十届联合国预防犯罪和罪犯待遇大会在一专题讲习班中讨论了计算机相关犯罪的影响。[1075] 讨论重点围绕犯罪类别、跨国调查以及针对这一现象的法律对策展开。[1076] 讲习班的结论中包含了目前仍在讨论的主要内容：需要予以刑事定罪、立法需要纳入程序性法律文书、国际合作至关重要、公私合作伙伴关系需进一步加强。[1077] 此外，讲习班还强调了能力建设的重要性 – 这一问题在此后的若干年内不断重提。[1078] 《维也纳宣言》呼吁预防犯罪和刑事司法委员会开展下列工作：

> *18* 我们决定就预防和控制计算机相关犯罪制定着眼于行动的政策建议，并邀请预防犯罪和刑事司法委员会在顾及其它论坛当前工作的同时开展以下工作。此外，我们亦将继续致力于提高自身预防、调查和控诉高科技及计算机相关犯罪的能力。

联合国大会第 55/63 号决议

同年，联合国大会通过了一项有关打击滥用信息技术进行的犯罪的决议，决议与 1997 年制定的八国集团《十点行动计划》有多点相似。[1079] 在此项决议中，联合国大会明确了一系列防止信息技术滥用的措施，其中包括：

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

第 55/63 号决议请各国采取必要措施，从区域和国际层面打击网络犯罪。这些措施包括：制定国内法律，杜绝滥用信息技术从事犯罪活动的“安全避风港”；提高执法能力，在查处滥用信息技术犯罪的国际案件中开展跨境合作；增进信息交流；提高数据和计算机系统的安全性；培训专业负责网络犯罪问题的执法人员；建设互助体制；以及提高有关网络犯罪威胁的公共意识。

联合国大会第 56/121 号决议

2002 年，联合国大会通过了另外一项关于打击滥用信息技术犯罪的决议。[1080]该决议提到了打击网络犯罪的现有国际方法，并突出强调了各类解决方案。

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

第 56/121 号决议强调，各国需要合作打击滥用信息技术的犯罪活动。决议还突出强调了联合国和其它国际及区域组织所能发挥的作用。决议进一步邀请各国在制定国内法律的同时考虑预防犯罪和刑事司法委员会的指导意见。

联合国大会第 57/239 和 58/199 号决议

第 57/239 和 58/199 号决议是有关网络安全问题的两项重要的联大决议。这两项决议回顾了第 55/06 和 56/121 号决议，并未探讨网络犯罪的细节。由于认识到各国在获取和使用信息技术方面的差距有可能降低在国际范围内合作打击滥用信息技术的犯罪行为的效率，因此，这两项决议进一步强调了在打击网络犯罪方面开展国际合作的必要性。[1081]

第十一届联合国预防犯罪和刑事司法大会

2005 年，在泰国曼谷举行的第十一届联合国预防犯罪和刑事司法大会（“联合国预防犯罪大会”）探讨了网络犯罪的问题。大会的背景文件[1082]和讲习班均提到了与使用计算机系统的新兴犯罪行为以及跨国犯罪规模相关的多项挑战。[1083]在大会之前召开的筹备会议框架下，埃及等多个成

员国要求就网络犯罪问题制定新的联合国公约，西亚地区筹备会议亦呼吁就新的公约开展磋商。[1084] 协商制定新公约的可能性还被纳入了第十一届联合国预防犯罪大会的讨论指南中。[1085] 然而，各成员国在此次大会上并未决定发起统一立法的行动。因此，《曼谷宣言》只是提到了现有的解决办法，并未提及具体的法律文书。

> *16* 我们注意到，处在当前全球化的时代，伴随着信息技术和新的电信与计算机网络系统的迅猛发展，出现了将这些技术滥用于犯罪目的的现象。因此，我们欢迎各国强化和补充现有的合作，推动对高科技犯罪和与计算机有关的犯罪的调查与起诉，包括与私营部门的合作关系。我们认识到联合国对有关打击网络犯罪的区域和其他国际论坛的重要贡献，要求预防犯罪和刑事司法委员会考虑到它的经验，检验在联合国和其他同样关注这些问题的组织的共同领导下为该领域提供进一步援助的可行性。

联合国大会第 60/177 号决议

第十一届联合国预防犯罪和刑事司法大会（2005 年，泰国曼谷）通过的《曼谷宣言》强调了协调一致、统一打击网络犯罪的必要性，[1086] 并提出了以下问题：

> 我们重申在犯罪问题上运用现有工具以及进一步开发国家措施和开展国际合作的重要性，如考虑强化和加大各种措施的力度，尤其是加强对网络犯罪、洗钱和文化产品非法贩卖的打击力度，以及就引渡、相互法律援助以及没收、回收和返还犯罪收益等开展合作。
>
> 我们注意到，处在当前全球化的时代，伴随着信息技术和新的电信与计算机网络系统的迅猛发展，出现了将这些技术滥用于犯罪目的的现象。因此，我们欢迎各国强化和补充现有的合作，推动对高科技犯罪和与计算机有关的犯罪的调查与起诉，包括与私营部门的合作关系。我们认识到联合国对有关打击网络犯罪的区域和其他国际论坛的重要贡献，要求预防犯罪和刑事司法委员会考虑到它的经验，检验在联合国和其他同样关注这些问题的组织的共同领导下为该领域提供进一步援助的可行性。

联合国大会第 60/177 号决议对 2005 年《曼谷宣言》表示赞同，宣言鼓励国际社会强化和补充现有的合作，以预防与计算机相关的犯罪活动，同时邀请各国进一步探寻在联合国和其他同样关注这些问题的组织的领导下为该领域提供进一步援助的可行性。

第十二届联合国预防犯罪和刑事司法大会

于 2010 年在巴西召开的第十二届联合国预防犯罪和刑事司法大会亦讨论了网络犯罪这一主题。[1087] 在四个区域的大会筹备会议（拉丁美洲和加勒比区域筹备会议 [1088]、西亚区域筹备会议[1089]、亚洲和太平洋区域筹备会议 [1090] 和非洲区域筹备会议 [1091]）中，各国呼吁就网络犯罪制定一项国际公约。相关学术机构也提出了类似要求。[1092]

大会过程中，各成员国在讨论计算机犯罪和网络犯罪问题过程中就联合国应该更加积极地参与打击活动取得了较大进展。大会代表就计算机犯罪和网络犯罪问题展开了为期两天的讨论，甚至为此专门组织了额外的边会，这些事实突出了这一主题的重要性，且此届预防犯罪大会围绕该主题展开的讨论要远比前两届大会激烈。[1093] 会议讨论主要围绕两个问题进行，即如何实现法律标准的统一以及如何协助发展中国家打击网络犯罪。如果联合国将制定综合的法律标准或建议成员国实施欧洲理事会《网络犯罪公约》，那么第一点将尤其重要。在筹备联合国预防犯罪大会过程中，欧洲理事会就联合国的措施表达了关切，[1094] 并呼吁对其《网络犯罪公约》予以支持。经过激烈的讨论 –

特别是针对《网络犯罪公约》有限应用范围的讨论，各成员国决定不建议批准《网络犯罪公约》，但建议联合国加强其在以下两个重要领域（已体现在《萨尔瓦多宣言》中）中的作用：

> *41* 我们建议联合国毒品和犯罪问题办事处根据请求，与成员国、相关国际组织和私营部门合作向各国提供技术援助和培训，以改进国家立法，建设各国当局的能力，以便打击网上犯罪，包括预防、发现、调查和起诉各种形式的此类犯罪，并增强计算机网络的安全。
>
> *42* 我们请预防犯罪和刑事司法委员会考虑召集一个不限成员名额的政府间专家组，对网上犯罪问题以及各会员国、国际社会和私营部门就此采取的对策进行一次全面研究，包括就国家立法、最佳做法、技术援助和国际合作开展信息交流，以期审查各种备选方案，加强现有并提出新的国家和国际打击网上犯罪的法律和其他对策。

因此，各成员国建议联合国毒品和犯罪问题办事处（UNODC）发挥有效作用，应要求提供全球能力建设。考虑到 UNODC 在刑事立法方面丰富的能力建设经验及其在全球范围内都设有区域办公室这一事实（这一点与欧洲理事会不同），将来，联合国有可能通过 UNODC 在这一领域内起到更加重要的作用。

第二点建议突出强调了各成员国未能在联合国预防犯罪大会上做出是否起草相关法律案文的决定。这也体现了大会讨论中存在的争议，会上，尤其是已经批准《网络犯罪公约》的欧洲国家均表示支持这一法律文书，而大量发展中国家却呼吁起草一项联合国公约。然而，各成员国还是做出了不同于第十一届预防犯罪大会的响应，未提出采用现有的法律文书，且更为重要的是，各成员国亦未建议将欧洲理事会的《网络犯罪公约》作为一项全球标准。相反，成员国建议联合国请预防犯罪和刑事司法委员会开展全面研究，在研究其它事项的同时审视打击网络犯罪活动的各项选择，包括强化现有立法，出台新的国际国内法律，或采取其它应对措施。

联合国大会第 64/211 号决议

2010 年 3 月，联合国大会通过了一项新的决议[1095]，以作为“培育全球网络安全文化”倡议的组成部分。第 64/211 号决议提到了两份有关网络犯罪[1096]的重要决议和两份有关网络安全[1097]的重要决议。决议的附件 – 国家保护重要信息基础设施努力资源评估工具 – 呼吁各国审查和更新由于新 ICT 迅速发展并且由于依赖这些新技术而可能过时或失效的法律依据（包括有关网络犯罪、隐私、数据保护、商业法、数字签名和加密的法律依据）。此外，该决议还呼吁各成员国在上述审查过程中利用区域和国际公约、安排和先例。

> *13* 审查和更新由于新 ICT 迅速发展并且由于依赖这些新技术而可能过时或失效的法律依据(包括有关网络犯罪、隐私、数据保护、商业法、数字签名和加密的法律依据)，在审查过程中利用区域和国际公约、安排和先例。确定贵国是否制定了调查和起诉网络犯罪的必要立法，注意到现有框架，例如联合国大会关于打击非法滥用信息技术的第 55/63 号和第 *56/121* 号决议和包括欧洲理事会《网络犯罪问题公约》在内的区域倡议。
>
> *14* 确定贵国有关网络犯罪的依据和程序，包括法律依据和国家防止网络犯罪部门的现状，以及检察官、法官和议员对网络犯罪问题的认识程度。
>
> *15* 评估现行法规和法律依据是否足以处理网络犯罪以及更广泛的网络空间当前和未来的挑战。
>
> *16* 检查贵国参与国际社会打击网络犯罪的努力，例如参加打击赛博犯罪全天候联络点网络的情形。
>
> *17* 确定在基础设施设在本国境内或罪犯居住在本国境内而受害者居住在其他地方的情形下，国家执法机构要求满足哪些条件，才与国际同行合作调查跨国网络犯罪。

自我评估工具的 18 项评估内容中有 4 项涉及网络犯罪，这一事实强调了旨在有效打击网络犯罪、维护网络安全的执法能力的重要性。

全球有关网络犯罪问题的研究

在针对联合国禁毒办有关网络犯罪的全面研究中的议题和方法[1098]进行了深入讨论[1099]后，2012 年初向联合国各会员国发出了一份调查问卷，同时亦开发了在线门户网站。[1100]问卷内容较为庞杂，其中涉及了与网络犯罪立法的不同层面相关的各种问题，如定义、刑事定罪和程序性文书等。在问卷中，会员国亦被要求介绍各自相关立法现状及不同区域性标准（如网络犯罪公约）的实施情况。相关回复结果已于 2013 年提交[1101]给联合国预防犯罪和刑事司法委员会。[1102]

2013 年，联合国毒品和犯罪问题办事处公布了首批研究结果。[1103]此项研究的复杂程度可谓前所未有，其中包含了 69 个会员国提供的回复结果。[1104]除来自会员国的回复外，研究亦纳入了对 40 多家企业和 16 家学术机构提交的 500 份可公开获得文件和资料的审查结果。研究强调，区域性协调文书（如欧洲理事会《网络犯罪公约》）的影响范围着实有限，并阐明了其他区域性文书的同等重要意义。[1105]专家工作组于 2013 年 2 月召开了会议，并将此问题提交给预防犯罪和刑事司法委员会。[1106]

2013 年 4 月，预防犯罪和刑事司法委员会首次就研究结果进行了讨论。[1107]第 22/7 号决议对已完成工作做了阐述，但并未提供更多详情。[1108]相反，委员会呼吁各会员国审议相关结果，并要求专家组继续开展工作，同时要求秘书处将研究结果翻译成联合国所有语文。在第 23 次会议期间，多位与会者就网络犯罪问题做了发言。[1109]尽管全球就此问题进行协调的呼声甚烈，但委员会并未就此做出决定。相反，委员会将侧重点放在了能力建设问题上，并重点推介了由联合国毒品和犯罪问题办事处运作的全球能力建设项目。[1110]

政府专家组

2013 年，政府专家组（其中包括来自爱沙尼亚、法国、德国和英国等欧洲国家的专家）提交了一份题为“国际安全背景下的信息和电信工作发展”的报告。[1111]网络/信息安全是工作组关注的焦点所在。此外，尽管工作组对相关常规进行了讨论，但对网络安全的一个具体问题（国家参与）却给予了特别专注。[1112]

有关网络犯罪问题的政府间专家组

根据各成员国呼吁 UNODC 建立政府间工作组的决定，工作组第一次会议于 2011 年 1 月在维也纳召开。[1113] 专家组由来自各成员国、政府间组织和国际组织、专业机构、私营部门和学术机构的代表组成。会议期间，专家组成员讨论了用于分析网络问题的全面研究框架草案和相应的对策。[1114] 就法律对策而言，多个成员强调了现有国际法律文书的实用性，这些法律文书包括《联合国打击跨国有组织犯罪公约》和欧洲理事会《网络犯罪公约》，此外成员还表达了制定一项专门应对网络犯罪问题的全球性法律文书的意愿。会议同意在完成上述研究之后决定是否应制定全球法律文书。

其它决议和行动

除此之外，联合国系统还通过大批决定、决议和建议应对网络犯罪问题，其中最为重要的举措如下所述：联合国毒品和犯罪问题办事处（UNODC）与网络犯罪和刑事司法委员会 [1115] 通过了一项关于打击对儿童进行性剥削的有效的预防犯罪和刑事司法对策的决议。[1116] 2004 年，联合国经济及

社会理事会（ECOSOC）[1117]通过了题为“开展国际合作，预防、侦查、起诉和惩处欺诈、滥用和伪造身份资料罪以及有关的犯罪”的决议。[1118] 2005 年，政府间专家组成立了一个工作组。[1119]此外还建立了一个处理身份相关犯罪问题的核心专家组，就该问题开展全面研究。2007 年，ECOSOC 通过了题为“开展国际合作预防、侦查、起诉和惩处经济欺诈和身份相关犯罪”的决议。[1120]虽然上述两项决议未能明确解决互联网相关犯罪的问题，[1121]但这两项决议仍然适用于此类犯罪行为。根据 ECOSOC 第 2004/26 号决议[1122]和 ECOSOC 第 2007/20 号决议[1123]，UNODC 于 2007 年建立了一个核心专家组，就最佳行动步骤交换观点。[1124]核心组已经开展了多项涉及互联网相关犯罪的研究。[1125] 2004 年，ECOSOC 通过了一项关于通过互联网销售国际管制合法药物的决议，该决议明确提到了与计算机相关的犯罪现象。[1126]

UNODC/国际电联谅解备忘录

2011 年，UNODC 和国际电信联盟（ITU）签署了一份有关网络犯罪的谅解备忘录。[1127]该谅解备忘录涉及合作（特别是能力建设和为发展中国家提供技术协助方面的合作）、培训和联合讲习班等内容。在能力建设方面，双方组织可以利用分布在各个大洲的数量众多的现场办事处。除此之外，双方组织还同意联合开展信息和知识传播以及数据分析。

5.1.3 国际电信联盟[1128]

作为联合国的一个专门机构，国际电信联盟（ITU）在电信标准化和发展以及网络安全问题方面起着领导作用。

信息社会世界高峰会议

此外，国际电联也是信息社会世界峰会（WSIS）的领导机构，该峰会分两个阶段进行 – 2003 年的瑞士日内瓦阶段峰会和 2005 年的突尼斯阶段峰会。来自世界各国的政府代表、政策制定者和专家就如何最好地应对全球信息社会发展带来的一系列问题交换了意见和经验，包括制定一致性的标准与法律。峰会的输出结果包含在《日内瓦原则声明》、《日内瓦行动计划》、《突尼斯承诺》以及《突尼斯信息社会议程》中。

《日内瓦行动计划》强调了采取打击网络犯罪相应措施的重要性：[1129]

> ***C5 树立使用信息通信技术的信心并确保使用的安全***
>
> *12* 信心与安全是信息社会的重要支柱。
>
> *[…]*
>
> *b)* 政府应当与私营部门合作，来防止、探测并响应网络犯罪和信息通信技术滥用现象，方法包括：制定指南，以便将各国在这些领域正在进行的工作考虑在内；考虑立法，以便对滥用行为进行有效的调查和起诉；促进有效的相互援助；在国际层面上加强制度支持，以便防止、探测和恢复此类事件；同时，鼓励对用户进行教育，提高其意识。
>
> *[…]*

2005 年在突尼斯召开的信息社会世界峰会第二阶段会议也提到了网络犯罪问题。《信息社会突尼斯议程》[1130]强调，在打击网络犯罪过程中需要开展国际合作，并参考现有的法律方法，如联合国大会的各项决议以及欧洲理事会《网络犯罪公约》等：

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

《全球网络安全议程》

作为信息社会世界峰会的一项成果，国际电联被指定为行动线 C5 的唯一促进机构，致力于树立使用信息通信技术的信心，并保证其安全。[1131] 在 2007 年召开的信息社会世界峰会行动线 C5 第二次促进会议上，国际电联秘书长强调了在打击网络犯罪的过程中开展国际合作的重要性，并宣布发布《国际电信联盟全球网络安全议程》。[1132] 《全球网络安全议程》由七大目标组成，[1133] 建立在五大战略支柱 [1134] 基础之上，包括为网络犯罪示范法的制定而精心制作的战略。这七大目标是：

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

2 为创建针对网络犯罪的适当的国家和区域组织结构和政策而精心制定战略。

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

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

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

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

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

为了分析《网络安全议程》的七大目标并制定相应的措施和战略，国际电联秘书长成立了一个高层专家组（HLEG），该高层专家组汇集了来自各成员国、业界以及科学领域的代表。[1135] 2008 年，专家组在进行磋商之后发布了“全球战略报告”。[1136] 报告中与网络犯罪最为相关的内容是第 1 章中的法律措施。除概要介绍打击网络犯罪的不同地域和国际方法之外，[1137] 该章内容还简要说明了相关刑事法律条款、[1138] 程序文书、[1139] 有关互联网服务提供商职责的规定 [1140] 以及保护互联网用户基本权利的保护措施。[1141]

能力建设

在国际电联《网络安全议程》的框架下，国际电联电信发展部门（ITU-D）协助各国在国家、区域和国际层面开展协调一致的网络安全相关活动。国际电联全权代表大会通过的第 130 号决议（2010 年，瓜达拉哈拉，修订版）强调了国际电联在能力建设方面的职责。根据这一决议，国际电联有责任协助成员国，尤其是发展中国家制定适合且可行的应对网络威胁的法律措施。

这些协助包括在制定国家战略、立法和执法以及组织结构（例如跟踪、预警和事件响应）等领域内开展能力建设活动。国际电联组织了若干次有关应对网络犯罪问题的区域性专题会议。[1142]

ITU-D 与来自公有和私营部门的合作伙伴一道，共同制定了网络安全/网络安全和关键信息基础设施保护（CIIP）工具，以协助成员国提升国家意识，开展国家范围的网络安全自我评估，修订相关法律以及提高跟踪、预警和事件响应能力。这些工具包括《了解网络犯罪：发展中国家的指南》、国际电联国家网络安全/CIIP 自我评估工具以及僵尸网络缓解工具包。

各项决议

在尚无法通过具体的刑事法律条款直接解决网络犯罪问题的情况下，国际电联通过了一系列涉及该问题的网络安全相关决议。

- 国际电联全权代表大会第 130 号决议（2010 年，瓜达拉哈拉，修订版） – 加强国际电联在树立使用信息通信技术的信心和提高安全性方面的作用。
- 国际电联全权代表大会第 149 号决议（2006 年，安塔利亚） – 研究与树立使用信息通信技术的信息和提高安全性相关的定义和术语。
- 世界电信发展大会（WTDC）第 45 号决议（2006 年，多哈） – 关于加强在网络安全、打击垃圾邮件等领域合作的机制以及关于加强在网络安全、打击垃圾邮件等领域合作机制的会议报告（2006 年 8 月 31 日 – 9 月 1 日）。
- 世界电信标准化全会关于网络安全的第 50 号决议（2008 年，约翰内斯堡，修订版）。
- 世界电信标准化全会关于抵制和打击垃圾信息的第 52 号决议（2008 年，约翰内斯堡，修订版）。
- 世界电信标准化全会第 58 号决议（2008 年，约翰内斯堡，修订版） – 重点鼓励发展中国家建立国家计算机事件响应组。

国际电联/欧盟在非加太国家共同资助的项目

为支持非加太国家政策和立法工作的发展，国际电联和欧盟决定共同资助一个项目[1143]，此项目亦为“非加太信息通信技术”和第九届欧洲发展基金的一部分。针对非洲、加勒比和太平洋地区的不同历史情况和重点任务，项目被细分为三个区域子项目。在撒哈拉以南的非洲地区，通过“非洲撒哈拉以南地区信息通信政策协调”项目（HIPSSA）提供了支持。在加勒比国家实施了“通过 ICT 政策、立法和监管程序的协调来提高加勒比地区的竞争力”（HIPCAR）项目。[1144]最后，针对太平洋地区的国家，则通过“支持太平洋岛屿国家的能力建设及信息通信技术政策、监管和立法框架（ICB4PAC）”项目提供了支持。

上述三个项目均包括两个主要阶段。第一阶段对现行法律进行了区域性评估，并与国际最佳做法进行了对比。在评估和深入磋商的基础上，示范政策和示范立法得以出台。第二阶段则向各国提供了支持，以在国家层面实现示范政策和示范立法的活学活用。

非洲撒哈拉以南地区信息通信政策协调（HIPSSA）

早在 2004 年，国际电联和欧盟即已启动一个区域性试点项目，以在西非促进综合 ICT 市场的建设（面向西非国家经济共同体/西非经货联盟的 ICT 市场协调）[1145]，并于 2005 年就此通过了一份最佳做法指南。[1146]为跟进此工作，2006 年[1147]，西非国家经济共同体的 ICT 部长们通过了统一的 ICT 监管决定；2007 年，西非国家经济共同体国家和政府首脑会议则通过了相关补充决定。[1148]

HIPSSA 则是上述试点项目的升级版。撒哈拉以南非洲的 42 个国家为项目受惠国。[1149]项目旨在通过一系列培训、教育和知识共享措施来制定和推广统一的 ICT 政策和导则，以营造一个可持续发展的市场环境[1150]，并促进 ICT 领域的人员和机构能力建设。

提高加勒比地区的竞争力（HIPCAR）

2008 年推出了面向 15 个加勒比国家的 HIPCAR 项目[1151]，以促进加勒比论坛（CARIFORUM[1152]）国家实现 ICT 政策和法律框架的统一。在筹备阶段共确定了 9 个工作领域[1153]，在项目第一阶段起草了示范政策和示范立法的案文，以在该地区促进统一立法的实现。相关工作领域包括：电子交易（商务）、电子证据、隐私和数据保护、通信截取、网络犯罪、公共信息获取/信息自由、普遍接入、互联互通及许可授予。为在国家层面实现示范政策和示范立法的活学活用，第二阶段则向多个国家（其中包括巴巴多斯、格林纳达、圣基茨和尼维斯、圣卢西亚和特立尼达）提供了支持。[1154]

支持太平洋岛屿国家的能力建设及信息通信技术政策、监管和立法框架（ICB4PAC）

应太平洋岛国要求推出的姊妹项目（ICB4PAC）[1155]则促进了与 ICT 政策和法规有关的能力建设，该项目重点针对 15 个太平洋岛国推出了培训、教育和知识共享措施，以促进这些国家在 ICT 领域的人员和机构能力建设。[1156]项目涵盖的工作领域包括许可和码号、普遍接入、互联互通、成本建模和网络犯罪等。

5.2 各区域的做法

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

5.2.1 欧洲理事会[1157]

欧洲理事会在应对网络犯罪威胁过程中发挥着积极作用。

1995 年之前开展的活动

1976 年，欧洲理事会（CoE）强调指出了计算机相关犯罪的国际特点，并且在一次涉及经济犯罪问题的会议上讨论了这一主题。该主题自此排上了欧洲理事会的议事日程。[1158] 1985 年，欧洲理事会任命了一个专家委员会[1159]，负责讨论计算机犯罪的法律问题。[1160] 1989 年，欧洲犯罪问题委员会批准了“关于计算机相关犯罪的专家报告”，[1161] 报告对打击新型电子犯罪（包括计算机欺诈和伪造）所需的实体刑法进行了分析。1989 年，部长委员会批准了一份建议书[1162]，建议书特别强调了计算机犯罪的国际特点：

> 根据《欧洲理事会规约》第 15.b 条的规定，部长委员会考虑到，欧洲理事会的目标是实现各成员国之间的更加紧密的团结；
>
> 意识到对与计算机有关的犯罪的新挑战作出适当而迅速反应的重要性；考虑到与计算机有关的犯罪常常具有跨国特点；意识到因此而需要进一步协调各国的法律和作法，并且为了促进国际法律合作，建议各成员国的政府：
>
> *1* 在评审本国的法律或者进行新的立法时，考虑到关于与计算机有关的犯罪的报告（此报告由欧洲犯罪问题委员会精心制作），尤其是要考虑到其中有关国家立法的指导方针；
>
> *2* 向欧洲理事会秘书长报告本国在 1993 年期间在与计算机有关的犯罪方面的任何法律、司法实践的进展情况以及国际法律合作的经验。

1995 年，部长委员会批准了另一份建议书，此建议书涉及跨国计算机犯罪引发的各种问题。[1163] 在建议书的附录中概述了有关起草适当法律的指导方针。[1164]

欧洲理事会《网络犯罪公约》及第一附加协议

1996 年，欧洲犯罪问题委员会（CDPC）决定成立一个负责应对网络犯罪问题的专家委员会。[1165] 在建立专家委员会之时，提出了通过另外一份建议书扩展响应原则并起草相应公约的意见。[1166] 1997 至 2000 年间，该委员会举行了十次全体会议、十五次开放起草小组会议。在 2001 年 4 月召开的委员会全体会议第二阶段会议上，大会批准了《网络犯罪公约》草案。[1167] 最终定稿的《公约》草案提交 CDPC 批准，随后，《公约》草案文本被提交部长委员会批准和签署。[1168] 于 2001 年 11 月 23 日在布达佩斯举行的签字仪式上，《公约》正式开放签字，共有 30 个国家签署了这一《公约》（包括四个非欧洲理事会成员国，即美国、加拿大、日本和南非，它们参与了谈判）。到 2014 年 6 月，共有 47 个国家 [1169] 签署、并有 42 个国家 [1170] 批准了 [1171] 欧洲理事会的《网络犯罪公约》（其中包括之前未签署公约的四个国家[1172]）。欧洲理事会共邀请 12 个国家[1173]加入《网络犯罪公约》，但这些国家仍未同意。[1174] 如今，《公约》被视为与网络犯罪作斗争的一种重要的国际手段，得到了不同国际组织的支持。[1175]

《网络犯罪公约》出台后，紧接着出台了《网络犯罪公约第一附加协议》。[1176] 在对《公约》文本进行谈判的过程中，对种族主义以及排外资料散布行为的定罪问题成为一个有争议的话题。[1177] 部分国家对言论自由原则 [1178] 采取严格保护，它们表达了相应担忧，即如果《公约》中包含的规定有悖其言论自由原则，那么它们可能无法签署《公约》。[1179] 在 1998 年出台的第四版草案中，《公约》中仍然包含一条规定，要求缔约方对“尤其涉及儿童色情制品和种族仇恨的”非法内容定罪。[1180] 为了避免部分国家出于言论自由的考虑而无法签署《公约》的情况，特在起草过程中将这些问题从《网络犯罪公约》中剔除，重新整合至一份单独的协议中。到 2014 年 6 月，已有 38 个国家 [1181] 签署、20 个国家 [1182] 批准了《附加协议》。

有关欧洲理事会《网络犯罪公约》的争论

目前，欧洲理事会《网络犯罪公约》仍然是一份已得到不同国际组织支持且覆盖范围最广的法律文书。[1183] 然而，第十二届预防犯罪大会上的争论强调，自《公约》开放签署以来已经过去十年，因此其影响已经有限了。[1184]

欧洲理事会《网络犯罪公约》的应用限制

截至 2011 年 1 月，美国是除欧洲国家外唯一一个批准了该文书的国家。像阿根廷、[1185]巴基斯坦、[1186] 菲律宾、[1187] 埃及、[1188] 博茨瓦纳 [1189] 和尼日利亚 [1190] 等国家虽未正式同意签署《网络犯罪公约》，但却将其作为示范并依据其起草了部分国家法律，因此无法完全通过签署或批准国家的数量衡量《公约》的影响。即使在上述国家中，也无法确定它们在何种程度上使用《公约》作为示范法。其中部分国家还使用了其它法律文本，例如关于攻击信息系统的欧盟指令和英联邦《网上犯罪示范法》。由于这些法律与《网络犯罪公约》存在大量的相似之处，且法律规定也很少逐字复制，而是根据各国的要求进行相应调整，因此，几乎完全无法确定是否使用以及在何种程度上使用《公约》作为导则。尽管如此，欧洲理事会声称已有 100 多个国家签署或批准《公约》，或在起草本国法律时使用《公约》作为示范法。[1191] 然而，这一数字无法予以核实。欧洲理事会没有披露这些国家的名称，只是提到有一份“内部名单”。更有甚者，准确的国家数量也从未披露过。即使能够证明确有 100 个国家使用了《网络犯罪公约》，这并不一定意味着这些国家的立法均与《公约》协调一致。欧洲理事会发布的这些模糊不清的信息还引发了有关《网络犯罪公约》的全部条款或仅仅某一条款是否得到实施的疑问。

批准速度

第十二届联合国预防犯罪大会不仅讨论了《网络犯罪公约》有限的区域覆盖问题，签署和批准速度也依然是会议关注的问题。自 2001 年 11 月 23 日有 30 个国家首次签署《网络犯罪公约》之后，九年之中仅有另外 17 个国家在《公约》上签字。且在这些国家中并不包含非欧洲理事会成员国，尽管欧洲理事会向八个非成员国家发出了邀请。[1192] 批准《公约》的国家数量分别如下：2002 年（2 个[1193]），2003 年（2 个[1194]），2004 年（4 个[1195]），2005 年（3 个[1196]），2006 年（7 个[1197]），2007 年（3 个[1198]），2008 年（2 个[1199]），2009 年（3 个[1200]），2010 年（4 个[1201]），2011 年（2 个[1202]），2012 年（6 个[1203]），2013 年（3 个）[1204]。与批准程序相比，实施程序也同样缓慢。一个国家从签署《公约》到批准一般需要 5 年以上。且不同国家在这方面的差异也很大。例如，在阿尔巴尼亚仅需要半年多时间即可批准《公约》，而德国却需要将近十年。

对于批准情况没有评估

到目前为之，欧洲理事会从未就提交批准文书的国家是否真正按照要求实施《网络犯罪公约》做出评估。特别是在那些最初批准《公约》的国家，《公约》是否得以完全实施仍然是一个重大顾虑。即使对于德国和美国这些大国而言，《公约》也未必得到全面实施。例如德国并未根据《公约》第 2 条的内容，对非法访问计算机系统的行为定罪，相反，只是规定非法访问计算机数据的行为属于犯罪行为。[1205] 欧洲理事会网站上公布的美国的网络犯罪立法国家资料显示，美国《民法典》第 18 章第 1030(a)(1) – (5) 款与《公约》第 2 条一致。[1206] 然而，与《网络犯罪公约》第 2 条不同的是，美国《民法典》第 18 章第 1030(a)款不仅仅对“访问”计算机系统的行为定罪，还对除“访问”计算机系统之外的其它行为（例如“获取”信息）做出了规定。[1207]

全球争论

《网络犯罪公约》广受诟病的一点便是其起草过程未充分考虑到发展中国家。[1208] 尽管网络犯罪具有跨国特点，但其对于世界各个区域的影响是不同的。对于发展中国家尤为严重。[1209] 《网络犯罪公约》不仅在磋商过程中缺乏亚洲、非洲和拉丁美洲地区发展中国家的广泛参与，还对非欧洲理事会成员国的参与设定了严格的条件，尽管其宗旨是面向非成员国开放的。根据《网络犯罪公约》第 37 条，加入《公约》需要征询所有缔约方的意见并获得其一致同意。此外，只有《公约》缔约方才可参与审议未来可能的修正。[1210] 第十二届联合国预防犯罪大会筹备框架下的争论表明，发展中国家尤其倾向于采取国际方法，而非通过加入区域性倡议解决网络犯罪问题。在第十二届联合国预防犯罪和刑事司法大会拉丁美洲和加勒比区域[1211]、西亚区域[1212]、亚洲和太平洋区域[1213]以及非洲区域[1214]筹备会议上，各国呼吁制定一项国际性的网络犯罪公约。同时，学术界也提出了类似倡议。[1215]

缺乏应对当前趋势的对策

网络犯罪属于不断发展变化的犯罪类型。[1216] 在《网络犯罪公约》制定之初的 20 世纪 90 年代，恐怖分子利用互联网[1217]、僵尸网络袭击[1218]和网络钓鱼[1219]等现象或者尚不为人知，或者未像当前一样严重[1220]，因此未能制定相应的具体解决方案。目前，欧洲理事会甚至也意识到《网络犯罪公约》已经有些过时。该结论可通过比较 2001 年时《网络犯罪公约》中有关儿童色情制品的条款和 2007 年的《保护儿童公约》证明。《保护儿童公约》第 20 (1)(f)条规定，“蓄意通过信息通信技术获取儿童色情制品”的行为属于犯罪行为。尽管使用信息通信技术已经表明该犯罪行为具有网络犯罪的性质，但《网络犯罪公约》却并未就该行为定罪。基于解释报告中提到的动机，起草者决定纳入该条款，以应对罪犯通过访问儿童色情网站而非通过下载相应内容的方式在线观看儿童影像的行为。因此，这意味着《网络犯罪公约》未涉及此类犯罪行为，在这方面甚至不符合欧洲理事会自身的现行标准。

程序性法律文书也同样具有这方面的问题。拦截 IP 语音（VoIP）通信、采用数字证据以及使用加密技术和匿名通信方式等新兴现象都属于非常重要但《网络犯罪公约》却没有提到的问题。在十年的续存期内，除有关仇外资料的附加协议外，《公约》从未进行修订，亦未增加任何额外的条款或法律文书。

随着技术和犯罪行为日益变化，刑事法律需要做出相应的调整。正如上文所述，网络犯罪立法要求在过去十年内已经发生了变化。因此，《网络犯罪公约》的更新势在必行。欧盟等区域性组织已经对近年来（约五年前）制定的有关网络犯罪的法律文书进行审议。尽管更新迫在眉睫，但更新过程却未必付诸实施。《网络犯罪公约》的强烈支持者 – 欧盟已在近期宣布其观点 – “更新《网络犯罪公约》[...]不能作为一项可行的选择方案。”[1221]

重点关注提供基础设施的国家而非发展中国家的参与

在过去十年，欧洲理事会未能吸引任何小国及发展中国家加入《网络犯罪公约》。原因之一在于《公约》在磋商过程中即缺乏发展中国家的参与。[1222] 尤为突出的是，亚洲和非洲国家的代表性不足，拉丁美洲更是无任何代表国家参与磋商。尽管欧洲理事会邀请了发展中国家的代表出席其重要的网络犯罪会议，但这些国家却不能参加审议未来可能的修正内容，原因在于审议会议仅限于《公约》缔约方参与。[1223]

与真正具有国际性的法律文书（例如联合国公约）相比，《网络犯罪公约》在加入程序方面也有所不同。尽管《公约》规定了缔约程序 – 旨在向非成员开放 – 但需要满足苛刻的条件。与联合国公约不同的是，加入欧洲理事会的《网络犯罪公约》需要与《公约》缔约国开展协商并获得其一致同意。[1224] 因此，在第十二届联合国预防犯罪大会上，发展中国家尤其呼吁采取一项（或多项）国际方法。在大会的拉丁美洲和加勒比区域 [1225]、西亚区域 [1226]、亚洲和太平洋区域 [1227] 以及非洲区域 [1228] 的筹备会议上，与会各国呼吁制定相应的国际性法律文书。

尽管欧洲理事会确立的重点关注西方国家的战略看上去是符合逻辑的，因为这些国家掌握着信息通信基础设施。然而如果关注重点中应该包含潜在受害者，那么发展中国家的参与便至关重要。2005 年，发展中国家的互联网用户数量超过了工业化国家。[1229] 排除发展中国家，仅仅关注（目前）提供了大部分基础设施和服务的发达国家这一做法忽略了两个重要方面：保护（大部分）互联网业务用户的重要性，以及印度、中国和巴西等新兴国家日益增加的影响力。如果不协助发展中国家制订相应的法律，以帮助他们针对影响本国的案件展开调查并与其它执法机构开展国际合作查找罪犯，那么当网络犯罪涉及这些发展中国家时，调查工作会更加困难。过去 10 年中没有一个发展中国家同意加入或批准《公约》这一事实体现了该区域方法的限制性。此外，欧洲理事会在过去十年中仅邀请了（未签署《公约》的 146 个联合国成员国中的）八个国家加入《公约》，这一点也突显了欧洲理事会在该领域投入的有限精力。这种现象自然与发展中国家在制定法律以及能力建设和技术援助方面的整体需求超出了《公约》自身机制这一事实有所关联。截至目前，欧洲理事会的工作重心只是协助各国保持国内相应法律与《公约》协调一致，而从未协助起草超出《公约》机制（例如弥合上述差距）的法律。此外，由于《公约》的实施还需要做出调整，因此有需要的国家可能已经就起草国内法律事宜寻求帮助了。例如，部分国家需要明确获准开展相应调查的单位（地方行政长官/检察院/警察局）以及调查依据（宣誓证据/宣誓证词/相关信息）。

第十二届联合国预防犯罪大会就这一问题展开了详细讨论，最终联合国各成员国决定加强联合国毒品和犯罪问题办事处（UNODC）在网络犯罪领域的能力建设职责。[1230] 国际电信联盟（ITU）等其它联合国组织机构已在近期接到了类似的指令。[1231]

不适合小国和发展中国家

小国和发展中国家在执行《公约》标准过程中面临诸多困难。欧洲理事会最小的成员国在过去十年中未批准[1232]《公约》这一事实清楚表明，执行《公约》不仅对于欧洲之外的小国是个挑战，对于欧洲小国亦是如此。

导致小国难以执行《公约》的规定之一便是需要建立 24/7 联络点。此类联络点对加快调查速度极为有用，因此，第 35 条便成为《公约》中最为重要的规定之一。[1233]然而值得一提的是，欧洲理事会于近期公布了一项分析国际合作在打击网络犯罪中的有效性的研究[1234]和一项关于 24/7 联络点在打击网络犯罪中的作用的研究[1235]，这两项研究的结果显示，并非所有批准《公约》的国家均建立了此类联络点，且即使已经建立联络点的国家也只是将其用于有限用途。

发展中国家面临的主要问题便是建立此类联络点属于强制性规定。对于发达国家而言，建立并维护此类联络点似乎并不困难，仅需要一支专业负责打击网络犯罪的警察队伍昼夜值班，然而对于专业打击网络犯罪的警力只有一名警察的国家而言，建立联络点无疑是一挑战。在这种情况下，履行该职责便需要大笔投入。因此，如同一名欧洲理事会代表近期在一次太平洋区域会议[1236]上声明的–加入和执行《公约》不会引发任何成本这一说法只有在排除一系列间接成本（例如维持 24/7 联络点或采用相应技术实时记录流量数据）的前提下才可谓准确。

没有普遍适用的途径

《公约》的重要目的之一便是提供一项能够解决网络犯罪领域所有问题的综合法律手段。[1237]但是通过与其它方法（特别是《英联邦计算机和计算机有关犯罪示范法》[1238]以及《电子商务指令》[1239]等欧盟法律文书）进行比较可以发现，《公约》忽略了非常重要的方面，例如有关电子证据的采用[1240]和互联网服务提供商（ISP）的义务的规定。特别是随着电子证据被普遍定义为新的证据类别，[1241]缺乏一项至少就电子证据采用的基础监管框架做出规定的条款将会引发严重后果。除非该国家已经另行制定了相应法律文书或该国法庭接受此类证据，否则，即使该国已经全面实施《公约》，仍无法为相应的罪犯判刑。

《保护儿童公约》

为了进一步保护未成年人免受性剥削，欧洲理事会在 2007 年出台了一项新的公约。[1242]在《保护儿童免受性剥削和性虐待公约》开放签字的第一天即有 23 个国家签署。截至 2014 年 6 月，签字国家数量已达 47 个，[1243]其中 31 个国家批准了该《公约》。[1244]《保护儿童公约》的关键宗旨之一便是实现各项保护儿童免受性剥削的刑法规定的一致性。[1245]为了实现这一目标，《公约》纳入了一系列刑事法律规定。除规定对儿童进行性虐待的行为属于犯罪行为（第 18 条）之外，《公约》还就交换儿童色情制品（第 20 条）和教唆儿童从事性目的活动（第 23 条）等行为做出了规定。

有关另一附加协议的谈判

早在 2012 年，网络犯罪公约委员会[1246]便通过了一份有关跨境接入和管辖权的报告。[1247]尽管各方对跨境接入问题投入了大量关注，但报告仍建议通过一项专门的附加协议。[1248]与网络犯罪公约谈判时所采用的闭门讨论方式不同，报告建议采用一种更加开放的磋商进程。[1249]2013 年 6 月，欧洲理事会发起了有关跨境接入的公众咨询。参与者所提供的报告显示，几乎所有专家对此均持批评态度，其中包括非政府组织、企业、欧洲理事国、欧盟各国和欧洲理事会的数据保护专家。[1250]

2013 年公布了有关跨境接入的工作组报告。[1251]报告列出了可能会加入附加协议的内容，其中涵盖了经同意的跨境接入以及未经同意的跨境接入等各种情况。[1252]2013 年 11 月则公布了与跨界接入有关的一份指导意见。[1253]

5.2.2 欧盟[1254]

在过去十年间，欧洲联盟（EU）制定了若干法律文件以解决网络犯罪问题。虽然这些法律文件在一般情况下只对 27 个成员国具有约束力，一些国家和区域正在将欧盟的标准作为本国和本区域讨论统一立法的参考文件[1255]。

2009 年 12 月之前的情况

在 2009 年之前，欧盟有关刑事法的权能有限并受到质疑。[1256] 除权能有限带来的挑战外，无法确定包括网络犯罪在内的有关刑法的权能是否由所谓“第一支柱”（欧洲理事会）或“第三支柱”（欧盟）[1257] 决定。由于人们普遍认为应由第三支柱负责，因此，只有在处理犯罪问题政策和司法合作的欧盟第三支柱内开展政府间合作的基础上才能实现统一。[1258] 2005 年，当欧盟法院在刑法领域宣布一个第三支柱法律文件（理事会有关通过刑法保护环境的框架决定[1259]）不合法时[1260]，权力分配首次受到质疑。法院做出决定，不可分割的框架决定违背了欧盟第 47 条，因为它侵犯了欧洲理事会通过第 175 条授予共同体的权力。该决定对有关统一欧洲联盟刑法的辩论产生重大影响。负责维护欧盟公约的欧洲理事会（EC）指出，通过评判发现，处理刑法的若干框架决定，完全或在一定程度上不正确，因为，其所有或一些条款是在不当法律基础上通过的[1261]。尽管承认仍有机会在第一支柱内评估权能，但是，由于第一支柱缺少对有关议题的处理，欧洲理事会的举措屈指可数。2007 年，欧盟法院通过法院第二号决定对比法律实践予以肯定。[1262]

《里斯本条约》批准后的情况

《里斯本条约》（“改革条约”）[1263] 于 2009 年 12 月生效，它大大改变了欧洲联盟的职能。除取消了“第一支柱”和“第三支柱”的区分外，首次在计算机犯罪领域为欧盟规定了严格的权能。《公约》有关欧盟运转（TFEU）的第 82 至 86 条规定了欧盟统一刑法（实体刑法和程序法）的权能。与网络犯罪最相关的条款是 TFEU 第 83 条[1264]。它授权欧盟制定与跨边界严重犯罪相关的罪行定义和制裁的起码规则。计算机犯罪在第 83 条第 1 段中被特别指出为相关犯罪领域之一。由于术语计算机犯罪的范畴超过网络犯罪，条约授权欧盟对两个领域予以监管。根据第 4 条第 2j 段，计算机犯罪法律的制定由欧盟和成员国共同负责。这使欧盟得以通过具有法律约束力的法令（第 2 条第 2 段）并将成员国行使权能的能力限制在欧盟尚未行使权限的领域。

在欧洲理事会于 2009 年通过的“斯德哥尔摩计划”中，欧盟强调将充分利用新的权能。[1265] 该计划确定了欧盟五年内在司法和内务领域的工作重点，是 2009 结束的“海牙计划”的延续[1266]。该计划突出了欧盟将发挥权能的打算，提到了 TFEU 第 83 条第 1 段指出的犯罪领域并将儿童色情和计算机犯罪作为工作重点。[1267]

欧盟法律文件和指导方针概述

尽管欧盟结构发生了根本性变化，过去通过的法律文件依然有效。根据《过渡条款议定书》第 9 条，基于《里斯本条约》生效前的欧洲联盟条约通过的法律文件须保留到这些法令被废除、废止或在执行中得到修正为止。因此，下一章概括阐述了所有相关欧盟法律文件。

一般性政策

早在 1996 年，欧盟就已经在一份有关处理互联网非法和有害内容的通讯中读到了有关互联网的风险。[1268] 欧盟强调成员国之间在打击非法在线内容方面开展合作的重要性。[1269] 1999 年，欧洲议会和理事会通过了有关促进更加安全地使用互联网并打击全球网络中非法和有害内容的行动计划。[1270] 该行动计划侧重于自律而非犯罪化。1999 年，欧盟还推出了“电子欧洲”举措，通过了欧洲理

事会题为“电子欧洲 – 面向所有人的信息社会”的通讯[1271]。该举措确定了主要目标，但未涉及对利用信息技术从事的非法行为的犯罪化。2001年，欧洲理事会（EC）发表了题为“通过提高信息基础设施的安全性和打击计算机犯罪搭建更加安全的信息社会”的通讯。[1272] 在此通讯中，欧洲理事会分析并探讨了网络犯罪的问题，同时指出，有必要为处理对信息系统和网络的完整性、可用性和可依赖性产生的威胁采取有效行动。

> 信息和通信基础设施已经成为我们经济中不可或缺的重要组成部分。遗憾的是，这些设施本身具有弱点，为犯罪分子实施犯罪活动提供了新的机会。这些犯罪活动可能采取多种多样的形式，并可能跨越多个国家。尽管出于种种原因，没有这方面的可靠统计数据，但毫无疑问，这些犯罪活动已经对行业投资和资产构成了威胁，也对信息社会的安全和信心构成了威胁。最近报告的有关拒绝服务攻击和病毒攻击的一些例子，已造成巨大的经济损失。
>
> 通过强化信息基础设施的安全性，以及通过确保执法机构拥有适当的执法手段，仍有机会来阻止犯罪活动，并同时充分尊重个人的基本权利。[1273]
>
> 委员会参与了欧洲理事会（*CoE*）和八国集团（*G8*）的讨论，认识到与程序法问题有关的复杂性和难度。但是，欧盟内部就与网络犯罪作斗争开展有效合作，是构建一个更加安全的信息社会并将网络世界建设成为一个自由、安全和公正的领地的至关重要的因素。[1274]
>
> 委员会将根据 *TEU* 的标题 *VI* 提出一些立法建议：
>
> […] 以便进一步在高科技犯罪领域接近实体刑法。这将包括那些涉及黑客攻击和拒绝服务攻击的违法行为。委员会还将详细审视旨在打击国际互联网上种族主义和排外行为的行动的范围，为的是依据 *TEU* 标题 *VI*，提出一个涵盖离线和在线种族主义和排外行为的框架决定。最后，还要审视国际互联网上非法药物的问题。[1275]
>
> 委员会将继续充分发挥作用，确保在其他国际论坛的各成员国间做好协调，这些国际论坛正对网络犯罪问题进行讨论，如欧洲理事会和八国集团等。在欧盟层面上，委员会的倡议将充分考虑其他国际论坛的进展情况，同时积极寻求进一步拉近欧盟内部的距离。[1276]

另外，2001 年，委员会发表了一篇关于“网络和信息社会”的通讯，[1277] 对网络安全问题进行了分析，并为在该领域采取的行动起草了一份战略纲要。

委员会的这两篇通讯都强调了需要在欧盟内部使各国的实体刑法更接近 — 尤其当考虑到针对信息系统的攻击。在与网络犯罪作斗争过程中，在欧盟内部对实体刑法进行协调被认为是在欧盟层面上所有举措的一个关键要素。 [1278]

2007 年，欧洲理事会发表了一篇有关打击网络犯罪的一般性政策的通讯[1279]。通讯概括了现状并强调了欧洲理事会《网络犯罪公约》作为打击网络犯罪的重要国际法律文件的重要性。此外，该通讯指出了欧洲理事会未来活动中重点处理的问题，其中包括：

在打击网络犯罪中加强国际合作。

- 在打击网络犯罪中加强国际合作。
- 为培训活动更好地协调财务支持。
- 组织执法专家会议。

- 加强与业界的对话。
- 监测不断变化的网络犯罪威胁以评估未来的立法需求。

电子商务指令（2000 年）

欧盟有关电子商务的指令[1280]除其它问题外处理的是互联网服务提供商（ISP）对第三方所从事行为承担的法律责任（第 12 条）。考虑到该网络国际性造成的挑战，起草者决定制定法律标准，为信息社会的全面发展提供框架并对整体经济发展以及执法机构的工作提供支持[1281]。由于信息社会服务的发展受到内部市场正常运转面临的若干法律障碍的影响，欧洲理事会因此获得权能[1282]。承担责任的规定基于责任分级原则[1283]。尽管该指令强调指出，无意统一该领域的刑法，但对刑法下的责任做出了规定[1284]。

理事会有关打击互联网儿童色情的决定（1999 年）

2000 年，欧洲联盟理事会采取措施解决互联网儿童色情问题。该决定的通过是对 1996 年有关互联网非法和有害内容的通讯[1285]和有关促进更安全的互联网的使用和打击全球网络中非法和有害内容的 1999 年行动计划[1286]的跟进。然而，该决定不包含通过具体刑法条款的义务。

欧洲理事会有关打击欺诈的框架决定（2001 年）

2001 年，欧盟通过了第一个直接针对网络犯罪问题的法律框架。欧盟有关打击欺诈和伪造非现金支付手段的框架决定[1287]包含围绕计算机欺诈具体问题和通过计算机程序等手段的制作用来从事框架决定[1288]所述罪行的刑法统一义务。

> **第 3 条–与计算机相关的罪行**
>
> 各成员国须采取必要措施，确认以下通过：为了从事犯罪行为的个人或第三方获得未经授权的经济利益故意从事或造成他人不当财产损失的货币或货币价值的转移为犯罪行为。
>
> — 未经授权的引入、修改、删除和废除计算机数据，特别是标识数据，或
>
> — 未经授权干扰计算机程序或系统的运转。

根据当时的普遍看法，又由于第一支柱缺少权能，法律文件是在第三支柱下制定的。文件强调指出，由于上述现象的国际性，这类问题是成员国自己无法彻底解决的。

欧洲理事会有关攻击信息系统的框架决定（2005 年）[1289]

在 2001 年发表了一般性政策后，欧洲理事会提出了制定攻击信息系统框架决定的提案[1290]。经过修改，理事会于 2005 年通过了该框架决定[1291]。同时，此文件被 2012 年指令取代（见下文）。尽管注意到该框架决定，欧洲理事会《网络犯罪公约》[1292]，它侧重于统一旨在保护基础设施的实体刑法条款。刑事程序法的内容（特别是调查和惩罚犯罪所必需的法律文件的统一）和有关国际合作的法律文件未整合至框架决定。决定突出了成员国在法律框架上的区别和差异以及有效应对信息系统攻击的政策和司法合作[1293]。

第 2 条–非法访问信息系统

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

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

第 3 条–非法系统干扰

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

第 4 条–非法数据干扰

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

数据保留指令（2005 年）

2005 年，委员会通过了欧盟数据保留指令[1294]。《指令》包含互联网服务提供商保存特定的通信流量数据的义务。这些数据对于识别网络空间中的违法犯罪人员是必不可少的。2014 年，欧洲法院宣布该指令无效。[1295]

第 3 条–数据保留的义务

1 为了部分废除 *2002/58/EC* 指令第 5 条、第 *6* 条和第 *9* 条，各成员国应采取一些措施来确保本指令第 5 条中规定的数据能够依照其条款的规定得以保留，所保留的数据指的是：由公众可用的电子通信服务提供商或者公共通信网络，在其管辖范围内、在提供有关通信服务时，产生或处理的数据。

2 第 1 段中规定的保留数据的义务应包括保留第 *5* 条中规定的数据，它们与不成功的呼叫尝试有关，在这些呼叫尝试中，由公众可用的电子通信服务提供商或者公共通信网络，在其管辖范围内、在提供有关通信服务时，产生或处理以及保存（关于电话数据）或记录（关于国际互联网数据）了这些数据。《指令》不得要求保留与未连接呼叫有关的数据。

指令将涵盖国际互联网上有关任何通信的关键信息这一事实，招致了人权组织的强烈批评，并可能导致对指令进行评审，将由立宪法院来实施评审[1296]。在西班牙音乐制作公司与西班牙电信的案件的接洽[1297]中，欧盟法院顾问、大法官 Juliane Kokott 指出，数据保留的业务可否在不违背基本权力的情况下得到执行令人质疑[1298]。八国集团于 2001 年就已强调了实施这类规定可能遇到的难题[1299]。

该指令基于欧洲理事会有关内部市场的权能（第 95 条）[1300]。起草者强调，区分与为调查网络犯罪而保留数据相关的法律和技术标准给内部电子通信市场带来障碍，使服务提供商面临隐含不同投资的需求[1301]。爱尔兰责成欧洲法院废除该指令并得到斯洛伐克的支持，因为该指令不是在适当的法律基础上通过的。两国认为，第 95 条不能作为充足的基础，因为该法律文件不侧重于内部市场的运转，而是将重点放在犯罪的调查、发现和惩罚上，欧洲法院以无根据的理由驳回诉讼，指出，保留数据义务的差别将直接影响内部市场的运转[1302]。法院进一步强调指出，这种情况表明共同体为统一规则的采用实现维护内部市场正常运转的目标制定立法的做法是合情合理的。

2014 年，欧洲法院最终宣布该指令无效。[1303]法院认为，该指令对个人隐私权和个人资料保护权等基本权利构成了各种严重干扰，且相关干扰未被限制在绝对必要层面。自此，各成员国均不再受该指令的约束，不过，因该指令衍生且已执行的国家法律则不会自动失效。目前尚不能确定的是欧盟是否将提出并通过一项新指令。

欧洲理事会打击恐怖主义框架决定的修正案（2007 年）

2007 年，欧盟开始讨论《关于与恐怖主义作斗争的框架决定的修正案草案》。[1304] 在修正案草案的引言中，欧盟强调指出，现有的法律框架对那些协助或者教唆和煽动恐怖主义的行为进行判罪，但并不对那些通过国际互联网散步恐怖主义技能的行为判罪。[1305] 有了这一修正案，欧盟正在积极采取措施，缩小差距，使整个欧盟的法律更接近《欧洲理事会关于预防恐怖主义的公约》。

第 3 条–与恐怖活动相关的犯罪行为

1 出于本框架决定的目的：

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

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

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

2 各成员国须采取必要措施来确保与恐怖相关的犯罪行为包含以下故意的行为：

(a) 公开煽动实施恐怖活动；

(b) 为恐怖主义招募人员；

(c) 为恐怖主义培训人员；

(d) 本着实施第 *1* 条 *(1)* 中所列举的某种行为的目的而恶意盗窃；

(e) 本着实施第 *1* 条 *(1)*中所列举的某种行为的目的而敲诈勒索；

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

3 对如第 *2* 段中所描述的可处罚的行为，并不是一定指实际实施的恐怖行为。

基于框架决定第 3 条，第 1（c）段，[1306]，当知道以下信息打算用于与恐怖活动有关的目的时，各成员国有责任对发布如何使用爆炸物的指南信息的行为予以判罪。需要找出这一信息的确打算用于与恐怖活动有关的目的的证据，很可能限制了法律条款的应用，原因是可以在国际互联网上找到大多数关于如何使用武器的指南信息，而它们的发布并不直接涉及恐怖攻击。由于大多数武器和爆炸物既可用于实施“普通”犯罪，也可用于实施恐怖活动（双重使用），因此，这一信息本身几乎不用能来证明发布它的人已经知道此类信息随后的用途。因此，需要考虑到信息发布的背景（例如，发布在由恐怖组织运营的某个网站上）。

有关儿童色情的指令（2011 年）

在《里斯本条约》批准后提交的第一个与网络犯罪相关的法律框架草案是于 2011 年通过[1307]的有关打击儿童性虐待和性剥削以及儿童色情的指令提案[1308]。起草者指出，信息技术可以使罪犯更加方便地制作并传播儿童色情内容[1309]，同时强调了利用具体规定应对挑战的重要性。指令实施国际标准，如《欧洲理事会保护儿童免受性剥削和性虐待公约》[1310]。

第 5 条–有关儿童色情的犯罪行为

1 成员国须采取必要的措施，确保第 2 至 6 段所述无权从事的有意行为受到惩罚。

2 购买和拥有儿童色情内容须最多受到至少一年监禁的惩罚。

3 利用信息通信技术故意获取儿童色情内容须最多受到至少一年监禁的惩罚。

4 传播、分发或传送儿童色情内容须最多受到至少两年监禁的惩罚。

5 提供、供应或准备儿童色情内容须以最多受到至少两年监禁的惩罚。

6 制作儿童色情内容须最多受到至少三年监禁的惩罚。

7 须由成员国决定该款是否适用于第 *2* 条第*(c)(iii)*段所述涉及儿童色情的案件，其当事人在当时已 *18* 岁或更大。

8 成员国须酌情决定该条款第 *2* 段和第 *6* 段是否适用于第 *2* 条第(c)(iv)段所述情况，由制作者制作并拥有的色情内容仅用于个人使用，第 *2* 条第*(c)(i)*、*(ii)*或*(iii)*段所述色情资料未用于制作，而且该行为不招致传播资料的风险。

与《公约》相同，该指令建议对通过信息通信技术手段获取儿童色情内容的行为判罪 [1311]。这使执法机构得以在可以证明犯罪人打开了具有儿童色情内容的网站但无法证明犯罪人下载了资料的案件中对犯罪人给予惩罚，如违规者使用密码技术在其存储媒介上保护下载文件 [1312]，收集证据将变得困难重重。有关《保护儿童公约》的说明性报告指出，条款还应适用于违规者仅在线观看儿童色情图片但并不下载图片的情况 [1313]。一般来说，打开网页就自动启动了下载程序 – 往往是在用户无知的情况下 [1314]。因此，条款主要适用于不下载资料的儿童色情内容的消费。这可以是在网站可以提供流视频并根据流体程序的技术配置不对所收到的信息进行缓冲但在传输后立刻废弃的情况 [1315]。

第 25 条–打击包含或传播儿童色情内容的网站的措施

1 成员国须采取必要措施，确保立即清除在其领土上托管的包含或传播儿童色情内容的网页并努力争取清除在其领土之外托管的这种网页。

2 成员国可采取措施，阻止其领土内互联网用户接入包含或传播儿童色情内容的网页。这些措施必需通过透明程序制定并提供充足的保障，特别确保实施必要和适当的限制，让用户了解限制的原因。这些保障还应包括司法赔偿的可能性。

除与儿童色情相关行为的犯罪化以外，初始草案包含规定成员国实施阻止包含儿童色情内容网站的义务的规定 [1316]。一些欧洲国家 [1317] 以及非欧洲国家，如中国 [1318]、伊朗 [1319] 和泰国 [1320] 使用了这种手段。有人担心，没有哪个技术理念被证明有效 [1321]，上述方法包含过分阻止的风险 [1322]。因此，强制性阻止已变化，由成员国决定各国是否应实施阻止义务。

有关攻击信息系统的指令（2013 年）

2010 年 9 月欧洲联盟提出了有关防止对信息系统的攻击指令提案 [1323]。该提案于 2013 年获得通过。[1324]如上述详细阐述的，欧盟于 2005 年通过了防止对信息系统攻击的框架决定 [1325]。提案说明备忘录强调，起草者的目的是更新并加强法律框架，以便通过对新的犯罪方式作出回应打击欧洲联盟的网络犯罪 [1326]。除 2005 年框架决定中对非法接入（第 3 条）、非法系统干扰（第 4 条）和非法数据干扰（第 5 条）的犯罪化，2010 年指令草案包含两项新的犯罪行为。

第 6 条 – 非法截获

成员国须采取必要措施，确保在无权的情况下通过技术手段从信息系统或在信息系统内对非公开计算机数据，包括从承载此类计算机数据的信息系统进行的电磁发射进行有意截获作为可受到惩罚的犯罪行为。

第 7 条– 犯罪使用的工具

成员国须采取必要措施，确保对于在有意和无权的情况下从事第 *3* 至第 *6* 条所述犯罪行为（非轻微犯罪案件），使用、进口、拥有、传播或提供以下工具之一的国际制作、销售和采购予以惩罚：

(a) 为实现第 *3* 至 *6* 条所述犯罪行为而设计或调整的计算机程序；

(b) 得以接入全部或部分信息系统的计算机密码、接入代码或类似数据。

两条规定在很大程度上符合《网络犯罪公约》的相应条款。

与欧洲理事会《网络犯罪公约》的关系

如上所述，欧洲理事会《网络犯罪公约》是在 1997 年至 2000 年期间谈判完成的。1999 年，欧洲联盟表达了有关《网络犯罪公约》的共同观点[1327]。它呼吁成员国支持欧洲理事会起草的《网络犯罪公约草案》[1328]。当时，欧盟自己没有制定类似法律框架的权能。《里斯本条约》的批准使情况发生变化。然而，欧盟目前尚未决定改变其有关《网络犯罪公约》的观点。在斯德哥尔摩计划中，欧盟不仅呼吁成员国批准《网络犯罪公约》，同时还指出，在欧盟看来，该公约将成为全球打击网络犯罪的法律框架参考[1329]。然而，这并非意味着，欧盟将拿出全面应对网络犯罪的手段，因为欧盟采用的方法有两大优势。首先，欧盟指令必需在很短的规定时限内得到实施，而欧洲理事会除政治压力外没有强制签署和批准公约的手段[1330]。第二，欧盟具有不断更新法律文件的情况，而欧洲理事会《网络犯罪公约》在过去 13 年中从未更新。

5.2.3 经济合作与发展组织[1331]

1983 年，经济合作与发展组织（OECD）启动了一项研究，研究关于对各国刑法进行国际协调的可能性，以便解决计算机犯罪问题。[1332] 1985 年，该组织发布了一份报告，分析了当前的法律，并提出了与网络犯罪作斗争的提议。[1333] 经济合作与发展组织推荐了一份最小的犯罪行为清单，对这些犯罪行为，各国应考虑予以判罪，如与计算机有关的欺诈、与计算机有关的伪造、更改计算机程序和数据以及截获通信等。1990 年，信息、计算机和通信政策（ICCP）委员会组建了一个专家组，以制定一系列有关信息安全的指导方针，这些指导方针到 1992 年起草完毕，之后 OECD 理事会批准了这些指导方针。[1334] 这些指导方针在制裁问题上包括以下几方面内容：

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

1997 年，在对这些指导方针进行评审后，ICCP 于 2001 年设立了第二个专家组来更新这些指导方针。2002 年，新版的指导方针《OECD 有关信息系统和网络安全的指导方针：着力培育安全文化》作为 OECD 理事会的一项建议书被采纳了。[1335]指导方针包含九条互补的原则：

1) 意识
参与者应意识到需要加强信息系统和网络的安全，并知道他们该如何加强信息系统和网络的安全。
2) 责任
所有参与者都有责任保证信息系统和网络的安全。
3) 响应
参与者应及时采取行动，并以合作的态度，来预防、侦查和响应安全事件。
4) 道德
参与者应尊重他人的合法权益。
5) 民主
信息系统和网络的安全应与民主社会的核心价值相一致。
6) 风险评估
参与者应进行风险评估。
7) 安全设计与实施
参与者应将安全视为信息系统和网络的一个不可或缺的重要要素。
8) 安全管理
参与者应采用一种综合方法来实施安全管理。
9) 再评估
参与者应对信息系统和网络的安全进行评审和再评估，并对安全政策、作法、措施和程序进行适当的修改。

2005 年，OECD 发表了一份报告，就垃圾邮件对发展中国家的影响进行了分析。[1336] 报告指出，与西方国家如 OECD 成员国相比，由于发展中国家的资源更有限、更昂贵，因此垃圾邮件的问题更加严重。[1337] 在收到联合国秘书长行政办公室战略规划部门发出的请求后，请求制定一份有关国际互联网用于恐怖主义目的的各国国内法律解决方案比较纲要后，2007 年，OECD 发布了一份有关各国国内法律如何处置“网络恐怖主义”的报告。[1338] 2008 年，OECD 发表了一份有关身份盗用的范围研究文件 [1339]。文件概述了身份盗用的特点、身份盗用的不同形式、有关受害者的问题和执法方案。文件强调指出，多数 OECD 国家没有使用具体条款解决问题的亲身经历，是否将身份盗用判为独立的罪行需要考虑。[1340] 2009 年，OECD 发表了有关恶意软件的报告 [1341]。尽管报告简要阐述了犯罪化问题，但重点是恶意软件的范围及其经济影响。

5.2.4 亚太经济合作组织[1342]

亚太经济合作组织（APEC）将打击网络犯罪确定为一项重要工作。APEC 领导人呼吁在从事打击网络犯罪的人员之间开展紧密合作 [1343]。2008 年在泰国曼谷召开的 APEC 电信和信息部长会议宣言突出了继续为打击网络犯罪而合作的重要性 [1344]。直至今日，APEC 尚未就网络犯罪制定法律框架。此外，APEC 在网络犯罪立法调查中认真研究了多国 [1345] 网络犯罪法律并开发了帮助各经济体制定和审议法律的方式数据库 [1346]。调查使用的问卷调查表《布达佩斯网络犯罪公约》规定的法律框架。

打击恐怖主义声明（2002 年）

2002 年，APEC 领导人发布了打击恐怖主义和促进增长的声明，已颁布有关网络犯罪的法律并加强国家网络犯罪调查能力[1347]。他们承诺在 2003 年 10 月之前努力颁布一套完整的有关网络安全和网络犯罪的法律，以便于国际法律文件保持一致，其中包括联合国大会第 55/63 号决议和欧洲理事会《网络犯罪公约》，此外，他们承诺指定各国负责网络犯罪的机构和国际高新技术援助联络点并在 2003 年 10 月前在没有这种能力的情况下开拓这种能力，同时建立交流有关威胁和漏洞评估的机构（如计算机应急响应小组）。

网络犯罪立法大会（2005 年）

APEC 组织了各种大会[1348]并呼吁参与打击网络犯罪的官员开展更加紧密的合作[1349]。2005 年，APEC 组织了网络犯罪立法大会[1350]。此次大会的主要目的是促进制定全面的法律框架以打击网络犯罪并提高网络安全性，帮助执法机构应对因技术进步产生的全新问题和挑战，促进区域内网络犯罪调查机构之间的合作。

电信和信息工作组

APEC 电信和信息工作组[1351]积极参与了 APEC 为提高网络安全性开展的工作[1352]。2002 年，该工作组通过了 APEC 网络安全战略[1353]。工作组通过参考现有联合国和欧洲理事会的国际作法[1354]表达了其有关网络安全立法的观点。电信和信息工作组电子安全任务组在 2003 年泰国召开的两场大会[1355]期间讨论了有关起草网络安全立法的经验。[1356]

5.2.5 共同体

网络安全是共同体探讨的问题之一。主要活动集中在立法的统一。统一共同体内立法和加强国际合作的工作受到以下因素的影响，共同体为处理有关该问题的国际合作至少需要达成 1 272 个双边条约[1357]。

考虑到网络安全不断提高的重要性，共同体各法律部长决定责成一个专家组基于欧洲理事会《网络犯罪公约》制定打击网络犯罪法律框架[1358]。专家组于 2002 年 3 月提交了报告和建议[1359]。2002 年晚些时候出台了有关计算机和计算机相关犯罪的模型法草案[1360]。根据专家组的明确指示以及对欧洲理事会《网络犯罪公约》作为国际标准的认可，该模型法在很大程度上符合上述公约确定的标准。然而，第 6 章将更深入地探讨其中的差异。

在 2000 年的会议上。小共同体辖区法律部长和大法官决定成立一个专家组，制定有关数字证据的模型法。该模型法于 2002 年出台[1361]。

除进行立法外，共同体组织了若干培训活动。共同体 IT 网络和发展（COMNET-IT）于 2007 年 4 月共同组织了有关网络犯罪的培训。

2009 年共同体第三国有关 ICT 的法律框架培训计划在马耳他实施，得到了共同体技术合作基金（CFTC）的支持。2011 年组织了另一项培训。

2011 年，共同体提出了“共同体网络犯罪举措”。该举措的主要目的是帮助共同体国家加强其有关政策、立法、监管、调查和执法的机构、人力和技术能力建设。[1362] 举措旨在使所有共同体国家在全球打击网络犯罪的活动中开展有效的合作。

5.2.6 非洲联盟

在 2009 年约翰内斯堡举办的非洲联盟通信信息技术部长特别大会中，各位部长探讨了有关在非洲国家加大使用 ICT 的各项议题。大会做出决定，非洲联盟委员会应与联合国非洲经济委员会一道为非洲各国制定一个法律框架，解决诸如电子交易、网络安全和数据保护的问题[1363]。

2011 年，非洲联盟提出了非洲联盟建立有关非洲网络安全的可靠法律框架公约草案[1364]。起草者的目的是加强各成员国有关信息通信技术的现有立法。有关职责，不仅局限于网络犯罪，还包含其它信息社会问题，如数据保护和电子交易。该公约比多数其它区域性手段更加全面。它包含四个部分。第一部分涉及电子商务。它探讨了货物和服务电子提供商的合同责任[1365]、电子形式的公约义务[1366]和电子交易的安全性等方面[1367]。第二部分涉及数据保护问题[1368]。第三部分有关打击网络犯罪。第 1 节包含 5 章，其中包括 6 个定义（电子通信、计算机化的数据、ICT 中的民族主义和仇外心理、儿童问题、儿童色情和计算机系统）[1369]。

第 III – 1 条:

在本公约中：

1) 电子通信指通过电子或电磁通信手段、标志、信号、书面资料、图片、声音或各种性质的消息向公众或部分公众进行的任何传输；

2) 计算机化的数据指，用计算机处理的以任何形式表示的事实、信息或概念；

3) *ICT* 中的民族主义和仇外心理指任何书面资料、图片或任何其它想法或理论的表达，宣传或鼓励针对一个人或一组人因民族、人种、祖先或国籍或民族或宗教产生的仇恨、歧视或暴力，从而成为民族主义和仇外心理的前提或动因；

4) 未成年人指《联合国儿童权力公约》规定的年龄小于十八（*18*）岁的人；

5) 儿童色情内容指任何性质或形式的数据，在视觉上体现为未成年儿童从事明显的性行为或表示未成年儿童从事明显性行为的实际图像；

6) 计算机系统指为执行一个程序而进行的部分或全部用于自动化数据处理的单独或非单独设备以及一系列互相连接的设备。

此外，第三部分探讨了制定国家安全政策和相关战略的必要性[1370]。第 2 章涉及法律措施的一般性问题。这包括有关合法机构的标准、民主原则、基本信息基础设施的保护、统一、双重犯罪和国际合作[1371]。第 3 章涉及国家网络安全系统的问题。这包括安全文化、政府的作用、公众私营伙伴关系、教育和培训以及公众意识的提高[1372]。第 4 章专门用来描述国家网络安全监测结构。第 5 章涉及国际合作。与诸如欧洲理事会《网络犯罪公约》等类似区域性框架的主要区别在于，《非洲联盟公约草案》（如无其它用于国际合作的途径）不得用于这种目的。第 21 和第 25 条中专门阐述了概念的不同。

***第 III – 1 – 21 条*: 国际合作**

各成员国须通过必要的措施，促进信息的交流和成员国各组织以及其他成员国类似组织数据的高速交流。这些组织负责将法律在双边或多边的基础上用于有关领土。

第 III – 1 – 25 条：国际合作模型

成员国须通过必要的措施和战略参与有关区域和国际网络安全的合作。（包括联合国、非洲联盟、欧洲联盟、八国集团等）在内的大量国际政府机构已通过旨在促进成员国参与这种关系框架的决议。国际电信联盟、欧洲理事会、共同体国家和其它组织已建立了国际合作模型框架，成员国可将此作为指导。

第三部分的第 2 节涉及实体刑法。第 1 节包含非法接入计算机系统[1373]、在计算机系统中非法保留[1374]、非法系统干扰[1375]、非法数据输入[1376]、非法数据截获[1377]和非法数据干扰[1378]的犯罪化。这些规定与其它区域采用的最佳做法 – 包括非洲采用的标准难分伯仲。举例而言，西非经济共同体（ECOWAS）指令草案与在计算机系统中的非法保留予以犯罪化[1379]。

第 III – 3 条：

非洲联盟各成员国须采取必要的法律措施，将以欺诈方式保留或企图将自己保留在部分或全部计算机系统中的情况确定为犯罪行为。

这是一个新的概念，但并非刑法条款，而是一项配合性措施。在此方面，其它区域性框架未提及，如企业提交其产品进行漏洞测试的义务。

第 III –7 条

[...]

2) 成员国须通过规则，要求 ICT 产品厂商提交其产品进行漏洞和担保测试，测试由独立专家进行，将所发现的上述产品中的任何形式的漏洞和建议解决问题的措施通报公众。

第 2 节包含为获利而进行的计算机相关造假[1380]、非法数据使用[1381]、非法系统干扰[1382]、数据保护违规[1383]、非法设备和犯罪组织[1384]的参与的犯罪化。[1385]

第 III – 9 条：

非洲联盟各成员国须采取必要的法律措施，将在知情情况下利用数据的行为确定为刑事罪行。

特别要指出的是，非法使用计算机数据的犯罪化已超出了多数其它区域法规文件确定的标准。

第 3 节涉及非法内容的犯罪化。非洲公约草案引入了制作和传播儿童色情内容[1386]、采购和进口儿童色情内容[1387]、拥有儿童色情内容[1388]、方便未成年人获取色情内容[1389]、传播民族主义或仇外心理资料[1390]、通过计算机系统[1391]进行民族主义攻击[1392]和拒绝或批准违背人权的屠杀或犯罪的犯罪化概念[1393]。

第 1 章最后一节包含广义处理有关网络犯罪的法律和电子证据的可接受性（“书面电子资料”）的规定。

第 III – 23 – 1 条：反网络犯罪法

各成员国须通过有效的立法措施，将影响 ICT 系统及其相关基础设施网络保密性、完整性、可用性和可生存性的行为确定为真正的刑事罪行，同时确定逮捕和惩罚罪犯的有效程序措施。呼吁成员国在必要情况下在国际网络犯罪立法模型中采用批准的语言，如欧洲理事会和共同体国家通过的语言。

第 III – 23 – 2 条:

非洲联盟各成员国须采取必要的立法措施，确保有关犯罪问题的书面电子资料的可读取性，以便按照刑法确定罪行，前提是这种书面资料已在判决前的辩论和讨论中提交，传播该资料的人员可得到适当确定，而且所述资料已在可以担保其完整性的条件下得到准备和保护。

特别有关第 III-23-1 条，起草者的目的不完全明确，因为第 1 章前几部分包含的犯罪定义为违背计算机系统完整性和可用性的罪行，因此，无法确定第 III-23-1 条（有关犯罪化）需要各国在多大程度上偏离非洲公约草案更详细阐述的罪行。

第二章包含旨在更新传统规定的条款，以确保在涉及计算机系统和数据时的适用性。它要求各国对使用信息通信技术 [1394] 从事的传统罪行，包括盗窃的财产犯罪行为、滥用信任或涉及计算机数据的勒索建立量刑制度 [1395]。更新包含传播确保使用数字电子通信的设施条款的犯罪化问题包含在内 [1396]，确保为国家安全利益保护机密的条款适用于计算机数据 [1397]。这种条款未包含在其它区域性框架内，有关第 III-24 条，无法确定计算机系统是否在传统的罪行中用于第一阶段（罪犯在闯入银行之前发送一个电子邮件，而不是拨打电话）将导致更严重的判决。

第 III – 24 条:

非洲联盟各成员国须采取必要措施，将使用 ICT 进行违反大陆法的行为，如盗窃、欺诈或拥有被盗物品、滥用信任、勒索钱财、恐怖活动、洗钱等作为更严重的罪行。

第 III-28 条 – 第 III- 35 条涉及债务和制裁。

第 III 节涉及程序法。它要求成员国得以保留计算机数据 [1398]、获得计算机数据 [1399]、加速保护 [1400] 并截获数据通信 [1401]。截至 2014 年 7 月，公约仍未获得通过。[1402]

5.2.7 阿拉伯联盟与海湾合作理事会[1403]

阿拉伯地区的许多国家已经采取了国家措施，并采用了一些方法来与网络犯罪作斗争，或者已经处于起草法律阶段。[1404] 这些国家的例子包括：巴基斯坦、[1405] 埃及 [1406] 和阿拉伯联合酋长国 [1407]（UAE）。阿拉伯联合酋长国向阿拉伯联盟提交了示范立法《打击 IT 犯罪指导法》以便协调该地区的立法。[1408] 阿拉伯内政部长理事会和阿拉伯司法部长理事会于 2003 年通过了该法律。[1409] 海湾合作理事会（GCC）[1410] 在 2007 年的会议上建议该理事会的成员国寻求一种考虑到国际标准的共同方法。[1411]

5.2.8 美洲国家组织[1412]

自 1999 年以来，美洲国家组织（OAS）一直在积极应对区域内的网络犯罪问题。其中，该组织在 REMJA 的管辖范围内举行了多次会议，REMJA 是美洲国家司法部长或部长或首席检察官的英文缩写。[1413]

政府间网络犯罪专家组

1999 年，REMJA 建议成立政府间网络犯罪专家组。专家组被责成完成对针对计算机和信息，或将计算机用作犯罪手段的犯罪活动的诊断；完成有关国家立法、政策和有关活动的诊断，确定具有专长的国家和国际实体并在美洲体系内确定打击网络犯罪的合作机制。

司法部长的建议

REMJA 在 2010 年前召开了八次会议[1414]。在 2000 年的第三次会议上，美洲司法部长或部长或大法官探讨了网络犯罪问题并就若干建议达成一致[1415]。这些建议包括支持考虑政府专家组在第一次会议上提出的建议，将其作为 REMJA 制定美洲打击网络安全风险战略文稿，该文稿文号为美洲国家组织大会第 AG/RES.1939/XXXIII-O/03)号决议。同时，请改组通过主席继续支持拟定战略。会议进一步建议指出，成员国应审议相互之间开展广泛有效合作的机制，以便打击网络犯罪并在可能的情况下研究加强技术和法律能力，从而加入到八国集团建立的，帮助开展网络犯罪调查的 24/7 网络之中。成员国被责成评估实施欧洲理事会《网络犯罪公约》的可行性并考虑加入该公约的可能性。除美国和加拿大于 2011 年签署了《网络犯罪公约》外，智力、哥斯达黎加、多米尼加共和国和墨西哥也在欧洲理事会的邀请下加入了公约。最后，呼吁 OAS 成员酌情审议并更新国内执法机构或组织的结构建议，以便顺应网络犯罪不断变化的性质，包括审议打击网络犯罪机构和提供传统治安或相互法律援助的各机构之间的关系。

美洲司法部长或部长或大法官在 2002 年召开的第四次会议建议，在 OAS 工作组跟进 REMJA 建议的框架内，网络犯罪政府专家组[1416]应重新组织起来并被授予跟进专家组拟定并由 REMJA-III 通过的建议的落实的职责，同时考虑拟定相关的美洲法律文件和模型法律，以便加强打击网络犯罪中的国际合作并考虑制定有关隐私、信息保护、程序问题和防止犯罪的标准。

司法部长第六次会议的建议[1417]包含一项进一步加强与欧洲理事会合作的呼吁，以便使 OAS 成员国考虑实施《网络犯罪公约》原则[1418]并遵守上述原则，同时通过实施必要的法律和其它措施。与此同时，会议建议进一步作出努力加强与网络犯罪领域内其它国际组织和机构的信息交流和合作，如联合国、欧盟、APEC、OECD、八国集团、共同体和国际刑警组织，以便使 OAS 成员利用上述机构取得的进展。此外，请成员国建立专门机构，调查网络犯罪，确定有关该问题的联络机构并加速交流信息获得证据，同时，加强政府机构和服务提供商以及其它提供数据传输业务的私营企业之间在打击网络犯罪方面的合作。

这些建议在 2008 年的会议上得到进一步重申[1419]。此次会议建议指出，考虑到专家组和以往 REMJA 会议通过的建议，各国考虑实施欧洲理事会《犯罪公约》原则并加入该公约，同时通过实施与必要的法律和其它措施。同样，会议建议在 OAS 总秘书处的领导下开展技术合作活动，通过法律事务秘书处和欧洲理事会继续加强与其它网络犯罪领域的国际组织和机构的合作，使 OAS 成员国利用其它组织取得的进展。最后，美洲打击恐怖主义秘书处（CICTE）和美洲电信委员会（CITEL）和网络犯罪工作组被责成进一步开展长期的协调和合作活动，确保实施 OAS 大会第 AG/RES.2004(XXXIV-O/04)号决议通过的全面的美洲网络安全战略。

2010 年，REMJA 在其第八次会议上[1420]探讨了网络犯罪问题。会议简单地讨论了继续整合和更新美洲通过 OAS 互联网网页开展打击网络犯罪合作的美洲门户并加强各国制定有关打击网络犯罪和电子证据的法律和程序措施的重要性。此外，会议强调，有必要加强与其它有关网络犯罪的国际组织和机构，如欧洲理事会、联合国、欧盟、APEC、OECD、G8、共同体和国际刑警组织交流信息和开展合作的机制，使 OAS 成员国得以利用上述实体取得的进展。

在 2012 年会议期间，司法部长们再次讨论了与网络犯罪有关的各类问题。[1421]与会者亦了解了特定网络犯罪单位的重要性。[1422]此外，部长们还呼吁成员国审查各自的法律制度，并在程序法、

电子证据和刑事审判等方面通过必要立法。[1423]会议还建议制定包含了反网络犯罪措施的网络安全战略，并进一步讨论了公民教育及对联合国预防犯罪大会的结果进行认可等问题。与早些年不同的是，在会议建议中并未要求各国批准网络犯罪公约，相反却采用了更为柔和的语言，并呼吁成员国“认识到以下考虑，即：某些美洲国家组织成员国已表示将适用欧洲理事会《网络犯罪公约》的原则，并加入……”。[1424]

2014 年会议[1425]所通过的建议与前几次会议保持了高度一致，而宣布将示范立法的制定工作纳入研究范围则堪称会议的一个新亮点。[1426]

5.2.9 加勒比地区

2008 年 12 月，国际电联和欧盟推出了“通过统一 ICT 政策、法律和监管程序加强加勒比地区的竞争力”（HIPCAR）项目，以促进加勒比地区 ICT 行业的发展[1427]。该项目构成“ACP-信息通信技术”和第九个欧洲发展基金的组成部分。受益国为 15 个加勒比国家[1428]。该项目的目的是帮助 CARIFORUM[1429] 国家统一 ICT 政策和法律框架。

在此项目中，确定了九个工作领域[1430]，分别制定了模型政策和模型法律文本以推进上述区域制定和统一法律。网络犯罪是九项工作领域之一。模型法律文本的制定分三个阶段。在第一阶段，收集和审议受益国现有法律。与此同时，确定区域和国际最佳做法，重点考虑直接可以在一些受益国使用的标准（如 2002 年共同体模型法）。然而，审议工作还包括对其它区域做法的审议，如欧盟和非洲。评估报告[1431]包含对现有立法的审议以及比较现有立法和区域和国际最佳作法的比较法律分析。为拟定一份差距分析，评估报告还确定了该区域的特殊需求（如有关打击垃圾信息的法律），这是国际最佳作法中不可或缺的。在 2010 年的研讨会中，与来自受益国的利益攸关各方讨论了评估报告[1432]。根据评估报告和差距分析，利益攸关各方起草了模型政策指南。

第二阶段兼顾政策指南制定了模型法案。在第二次讲习班中，政策专家、法律起草者和其他来自受益国的利益攸关各方讨论并修改了为本次会议拟定的模型立法案文草案并通过了该草案。模型立法案文有三个主要目的：它提供了符合国际最佳作法的具体样本语言，它反映出了该地区的特殊需求并按照该地区法律起草作法制定以确保顺利实施。模型立法案文包括一套复杂的定义和具体的刑法条款，包括处理诸如垃圾信息的规定。这些问题对该地区来说至关重要，但不一定包含在其它区域框架中，如欧洲理事会《网络犯罪公约》。

15. (1)一个无合法缘由或理由的人:

a) 有意从或通过这种计算机系统启动或传输多个电子邮件信息，或

b) 使用受保护的计算机系统转接或转发多个电子邮件信息，以便欺骗或误导用户或任何电子邮件或互联网服务提供商这种消息的来源，或

c) 真正篡改多份电子邮件信息中的字头信息并有意启动这种消息的传输犯下应受到惩罚的罪行，受到监禁不超过[时间]或罚款不超出[数量]的判决或同时受到双重惩罚。

(2) 国家可将传送多电子消息的犯罪限制在客户或商务关系中。各国可决定在第 15 (1) (a) 节中不对此行为罪犯化，前提是存在其它有效补救措施。

此外，该案文包含程序法规定（包括先进的调查手段，如使用远程取证手段）和有关互联网服务提供商（ISP）的责任的规定。

5.2.10 太平洋地区

除国际电联和欧盟共同赞助的加勒比地区的项目外，上述组织在太平洋地区推出了一个项目（ICB4PAC）[1433]。该项目旨在基于太平洋岛国的要求提供有关 ICT 政策和立法的能力建设。在此方面，项目侧重于提高 ICT 领域的人力和机构能力，开展培训、教育和知识共享措施。受益国为 15 个太平洋岛国 [1434]。2011 年 3 月，有关当前太平洋区域网络犯罪立法的讲习班在瓦努阿图举行 [1435]。讲习班介绍了对该地区现有立法的全面比较性法律分析以及与其它区域最佳作法的比较 [1436]。作为对此讲习班的跟进，有关制定网络犯罪政策和立法的大会于 2011 年 8 月在萨摩亚举行 [1437]。大会介绍了来自其它区域的最佳作法并制定了统一政策和立法结构。大会探讨了具体的刑法、程序法、国际合作、互联网服务提供商（ISP）责任、电子证据和防止犯罪措施。

2011 年 4 月，太平洋社会理事会组织了有关打击太平洋地区网络犯罪的大会 [1438]。该活动是与欧洲理事会共同组织的。大会探讨了有关具体刑法、程序法和国际合作的问题 [1439]。

5.2.11 南部非洲发展共同体（SADC）

南部非洲发展共同体（SADC）通过的示范立法采用了与非洲联盟类似的工作方法。该示范立法阐述了数据保护[1440]、电子商务[1441]和网络犯罪等问题。[1442]

5.3 科学和独立的方式

5.3.1 斯坦福国际公约草案

制定有关全球范围内网络犯罪法律框架的最著名的科学方式要数《斯坦福国际公约草案》（“斯坦福草案”）[1443]。斯坦福草案是作为对 1999 年斯坦福大学主办的大会的跟进 [1444]。与欧洲理事会《网络犯罪公约》的比较 [1445] 显示出一系列相同性。二者均涉及实体刑法、程序法和国际合作。主要的区别是，斯坦福草案制定的罪行和程序手段只适用于对信息基础设施的攻击和恐怖袭击，而欧洲理事会《网络犯罪公约》提到的程序法和国际合作手段还可适用于传统的罪行 [1446]。

5.3.2 全球网络安全和网络犯罪议定书

2009 年在埃及召开的互联网管理论坛中，Scholberg 和 Ghernaouti-Helie 介绍了有关全球网络安全和网络犯罪议定书提案 [1447]。第 1-5 条涉及网络犯罪并建议实施具体的刑法规定、程序法规定、针对互联网恐怖滥用的措施、有关全球合作和信息交流的措施以及隐私和人权措施 [1448]。议定书附录中规定的模型法在很大程度上（第 1-25 条）基于欧洲理事会《网络犯罪公约》规定的条款措辞。

2014 年 6 月，Scholberg 提交了有关针对网络空间设立国际刑事法院或法庭的联合国条约草案第 9 版[1449]，其中所建议的科学方法并不以正式的联合国授权为基础，而是凸显了网络空间在管辖权方面所面临的挑战。此外，草案亦提出了一个国际法庭的概念，该法庭将具有与常设国际法庭可比的有限管辖权。

5.4 不同国际与法律方法之间的关系

在技术协议方面单一标准的成功施行提出了一个问题，那就是：如何避免不同国际方法之间的冲突。[1450] 欧洲理事会《网络犯罪公约》和共同体《网络犯罪示范法》是最综合方式的框架，因为，它们涉及实体刑法、程序法和国际合作。但上述法规均未修正以应对近来的发展。此外，上述

两部文书的范围有限。上届联合国犯罪大会突出了国际法律文件中国家的利益。[1451] 由此引发了现有区域手段与可能的国家行动之间的关系，现存在三种可能的关系。

如新的立法手段确定了与区域和国家层面现有方式不同的方法，这样至少可以对必要的统一程序产生不良影响。因此，很可能新的手段对现有标准进行认真分析，确保一致性。举例而言，非法接入的犯罪化是共同体有关网络犯罪模型法第 5 节和欧洲理事会《网络犯罪公约》第 2 条以类似方式确定的。

此外，新的手段可以避免将导致实施困难或甚至使各国无法加入法律文件的条款包含在内。一个例子就是在欧洲理事会《网络犯罪公约》第 32b 条中探讨的有争议性的规定。该条款在网络犯罪委员会 2007 年会议上受到俄罗斯代表团的批评 [1452]。

最后，新的国际手段除包含不同法律手段中相同的基本标准外 – 侧重于差别分析以确定未充分探讨的领域，由此，将一些网络犯罪行为犯罪化并确定现有法律文件尚未包含的程序文书。2001 年以来已取得明显进展。当欧洲理事会《网络犯罪公约》起草时，“钓鱼”[1453]、“身份盗窃”[1454]和有关在线游戏和社交网络的行为仍不相关。新的国际手段应继续通过加入具有跨国特点的行为统一程序 [1455]。

5.5 国际与国家法律方法之间的关系

正如此前所指出的那样，网络犯罪是一种真正的跨国犯罪。[1456] 一般地，攻击者可以瞄准世界任何国家的用户进行打击，基于这一事实，执法机构之间开展国际合作是对国际网络犯罪进行调查的一项基本要求。[1457] 调查需要合作手段，并有赖法律协调。由于双重犯罪这一公共原则，[1458] 有效的合作首先要求对实体刑法规定进行协调，以防止出现“安全避风港”。[1459] 此外，需要协调调查手段，以确保国际调查涉及的所有相关国家都具有所需的调查手段，以便完成调查工作。最后，执法机构之间的有效合作要求采用与实际问题有关的有效程序。[1460] 因此，协调联动机制的重要性以及在全球协调过程中联合参与的需求，对任何国家的反网络犯罪战略而言，即使不是一种必然，至少也是一种趋势。

5.5.1 国家方法得以普及的原因

尽管国际社会广泛认可协调的重要性，但执行国际法律标准的过程远未完善。[1461] 为什么国家方法在与网络犯罪作斗争的过程中起着重要作用？其中一个原因是犯罪活动的影响并非普遍相同。国家方法的一个例子是在反垃圾邮件斗争中所采取的方法。[1462] 涉嫌垃圾邮件的电子邮件对发展中国家的影响尤其严重，对该问题，在经济合作与发展组织（OECD）的一份报告中进行了分析。[1463] 由于发展中国家的资源更稀少、更昂贵，因此与西方国家相比，垃圾邮件对发展中国家的影响要严重得多。[1464] 网络犯罪的影响不同，加上现有法律结构和惯例的差别，是众多国家层面的法律措施不执行或者只是部分执行国际标准的主要原因。

5.5.2 国际解决方案对国家解决方案

在技术全球化的时代，这种讨论看起来有点奇怪，原因是任何希望连接国际互联网的人都需要利用一些适当的（技术）标准协议。[1465] 单一的标准是网络运营的一项基本要求。不过，不像技术标准，法律标准仍存在差异。[1466] 在网络犯罪国际化的趋势下，它必须回答国家方法是否依然适用这个问题。[1467] 这一问题与用于执行不符合现有国际标准的法律的所有国家和区域方法都相关。缺乏协调可严重阻碍国际调查，而那些国际标准之外的国家和区域方法，可在实施国际调查中避免问题和困难。[1468]

区域和国家方法日渐增多，有两个主要原因。首先是立法速度。欧洲理事会既不强迫任何成员国签署《网络犯罪公约》，也不强迫《公约》签署国批准它。因此，与国家和区域法律方法相比，协调过程常常看起来比较慢。[1469] 与欧洲理事会不同，欧盟采取了一些方法来强迫各成员国执行框架决定和指令。这就是为什么 2001 年签署了《网络犯罪公约》但尚未批准它的许多欧盟成员国仍执行 2005 年欧盟理事会关于信息系统攻击的框架决定的主要原因。

第二个原因与国家和区域差异有关。有些违法行为只在区域中的某些国家才会被定罪。这方面的例子是宗教违法行为。[1470] 尽管要对有关涉嫌侮辱宗教符号的违法行为的刑法条款进行国际协调看起来是不可能的，但在这方面，国家方法可以确保某国的法律标准得以维持。

5.5.3 国家方法的困难

国家方法面临许多问题。至于传统犯罪，一个或几个国家对某些行为的判罪，可以严重影响违法者在这些国家进行违法活动的能力。不过，当涉及与国际互联网有关的违法行为时，单个国家对违法者的影响力将大打折扣，原因是，在通常情况下，只要连接到国际互联网，违法者就可以从世界任何地方进行其违法活动。[1471] 如果他们从并不对这些行为判罪的某个国家实施违法行为，那么国际调查以及引渡请求常常会失败。因此，国际法律方法的关键目标之一是通过规定和采用全球标准，防止出现对违法者而言是安全的“避风港”。[1472] 因此，一般地，国家方法需要采用额外的辅助措施，使之能够发挥作用。[1473]这些最普遍的辅助措施为：除了对非法内容的提供商判罪以外，还对其使用者进行判罪，对在犯罪实施过程中使用的服务判罪。

除了对非法内容的提供商判罪以外，还对其使用者进行判罪

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

对在犯罪实施过程中使用的服务进行判罪

第二种方法是管制，甚至在管辖范围内对某些用于犯罪目的的服务进行判罪。这一解决方案胜于第一种方法，原因是它牵涉提供中性服务的企业和组织，这些中性服务既可用于合法行为，也可用于非法行为。这种方法的一个例子是美国于 2006 年制定的《非法国际互联网赌博强制法案》。[1474]

与这一措施密切相关的是，确定对国际互联网上可用的某些内容进行过滤的义务。[1475] 在著名的雅虎（Yahoo）决定中，[1476] 就曾讨论过这一方法，而且这一方法目前正在以色列展开讨论，该国的接入提供商有义务限制访问某些含有成人内容的网站。对国际互联网内容实施控制的尝试不仅仅限于成人内容；一些国家还利用过滤技术来限制对涉及政治主题的网站的访问。开放网络倡议 [1477] 报告说，大约有二十四个国家实施了这种审查制度。[1478]

[1047] This includes regional approaches.

[1048] The Group of Eight (G8) consists of eight countries: Canada, France, Germany, Italy, Japan, United Kingdom, United States and the Russian Federation. The presidency of the group, which represents more than 60 per cent of the world economy (source: http://undp.org), rotates every year.

[1049] The idea of the creation of five subgroups – among them, one on high-tech crimes – was to improve implementation of the 40 recommendations adopted by G8 Heads of State in 1996.

[1050] The establishment of the subgroup (also described as the subgroup to the "Lyon Group") continued the efforts of the G8 (at that time still G7) in the fight against organized crime, which started with the launch of the Senior Experts Group on Organized Crimes (the "Lyon Group") in 1995. At the Halifax summit in 1995, the G8 stated: "We recognize that ultimate success requires all Governments to provide for effective measures to prevent the laundering of proceeds from drug trafficking and other serious crimes. To implement our commitments in the fight against transnational organized crime, we have established a group of senior experts with a temporary mandate to look at existing arrangements for cooperation both bilateral and multilateral, to identify significant gaps and options for improved coordination and to propose practical action to fill such gaps". See: Chairman's Statement, Halifax G7 Summit, June 17 1995. For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1051] Regarding the G8 activities in the fight against cybercrime, see also: United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1052] "Communiqué of the Ministerial Conference of the G8 Countries on Combating Transnational Organized Crime", Moscow, 19-20 October 1999.

[1053] 14. As the use of the Internet and other new technologies increase, more criminals are provided with opportunities to commit crimes remotely, via telephone lines and data networks. Presently, malicious programming code and harmful communications (such as child pornography) may pass through several carriers located in different countries. And infrastructures such as banking and finance increasingly are becoming networked and thereby vulnerable to cyber-attack from distant locations. We convene today to provide additional personal attention to and direction for our joint action against this transnational criminality.

15. Our goals are to ensure that our people are protected from those who use new technologies for criminal purposes, such as child exploitation, financial crime, and attacks on critical infrastructures, and to ensure that no criminal receives safe haven anywhere in the world. We are determined that our law enforcement authorities have the technical ability and legal processes to find criminals who abuse technologies and bring them to justice. The safety of our people and their economic prosperity depend upon our leadership and determination and our ability to take coordinated action. We direct our experts to continue their work, particularly, on problems which arise for our law enforcement authorities from new developments in information technology and their use by criminals.

16. Strength of G-8 Legal Systems. Our experts have completed a comprehensive review of G-8 legal systems to assess whether those systems appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes. While, over the past decade, our governments have acted to see that their legal systems account for new technologies, there remains room for improvement. Where laws or legal processes require enhancements, we are committed to use best efforts to fill these gaps and, consistent with fundamental national legal principles, to promote new legal mechanisms for law enforcement to facilitate investigations and prosecutions.

17. Principles on Transborder Access to Stored Computer Data. Criminals take advantage of the jurisdictional inability of law enforcement authorities to operate across national borders as easily as criminals can. High-tech crimes may rapidly affect people in many countries, and evidence of these crimes, which may be quickly altered or destroyed, may be located anywhere in the world. Recognizing these facts, and taking into account principles relating to sovereignty and to the protection of human rights, democratic freedoms and privacy, our law enforcement authorities conducting criminal investigations should in some circumstances be able to pursue investigations across territorial borders. We have today adopted certain principles for access to data stored in a foreign state, which are contained in the Annex 1 to this Communique. We are committed to work towards implementation of these principles through international cooperation, including legal instruments, and through national laws and policies, and invite all nations to join in this effort. We note, however, that continued work is required in this area, including on the appropriate collection, preservation and disclosure of traffic data, and we direct our experts to make further progress in consultation with industry.

18. Locating and Identifying High-tech Criminals. To ensure that we can all locate and identify criminals who use networked communications for illegal purposes, we must enhance our ability to trace communications while they are

occurring and afterwards, even when those communications pass through multiple countries. Existing processes are often too slow and are designed more to address bilateral cooperation than crimes requiring the immediate assistance of many countries. Faster or novel solutions must be found. We, as Ministers, direct our experts to develop, in consultation with industry, a concrete set of options for tracing networked communications across national borders in criminal investigations and provide those options as soon as possible within one year.

19. International Network of 24-hour Contacts. Our 24-hour points of contact network, which allows us to respond to fast-breaking investigations, has now been expanded from the eight G-8 countries to a number of additional countries around the world. The speed of electronic communications and perishability of electronic evidence requires real-time assistance, and this growing global network has dramatically increased our investigative abilities. We direct our experts to facilitate further growth of this network. G-8 nations and their partners should also use this network proactively to notify other countries when they learn of significant potential threats to our shared networks.

20. Criminality Associated with the 'Millennium Bug'. Our countries have been at the forefront of efforts to successfully tackle the 'Millennium Bug' or 'Y2K Problem', which presents a major threat to the increasingly networked global economy. We are concerned that the Millennium Bug may either provide new opportunities for fraud and financial crimes, or mask ongoing criminality, if systems for accounting and reporting are disrupted. Therefore, as part of our new proactive use of our 24-hour network, we will provide early warning of Y2K-related abuses.

21. Internet Fraud. We recognize that Internet fraud, in all of its forms, poses a significant threat to the growth and development of electronic commerce and to the confidence that consumers place in electronic commercial transactions. To counter this threat, we are undertaking a comprehensive response, including crime prevention, investigation, and prosecution. For example, we are sharing information on international Internet fraud schemes – including information relating to the criminals, their methods and techniques, the victims involved in these schemes, and reports of enforcement actions – so that criminals defrauding people in multiple countries are investigated and prosecuted for the full range of their criminal activities.

[1054] The idea of a 24/7 network has been picked up by a number of international approaches in the fight against cybercrime. One example is Article 35 of the Convention on Cybercrime:

(1) Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a) the provision of technical advice;

b) the preservation of data pursuant to Articles 29 and 30;

c) the collection of evidence, the provision of legal information, and locating of suspects. […]

[1055] *Jean-Pierre Chevenement*, the French Minister of the Interior, stated: "Now that the G8 has provided the impetus, it's vital that we formalize the new legal rules and procedures for cooperation in a legal instrument applying world-wide. For France, the negotiations under way in the Council of Europe on a Convention on Cyber-Crime are of fundamental importance for several reasons. The draft currently under discussion defines the offences which all States would have to recognize. It goes on to propose ways in which they could cooperate, taking up, for example, the idea of national contact points. It also proposes extradition procedures. In short, this agreement is an essential instrument, which France wants to see concluded within a reasonable period of time. The important thing about these negotiations is that the countries involved include some major countries outside the Council of Europe and that, once signed, this convention will be opened for signature by all States wishing to accede to it. The idea is in fact to get a convention which applies world-wide so that there can be no more "digital havens" or "Internet havens" in which anyone wanting to engage in shady activities can find all the facilities they need, including financial ones, for laundering the product of their crimes. Since we must never lose sight of the fact that the Internet is a global system and that no country can isolate itself from the rules under which it has to operate."

[1056] G8 Government-Industry Workshop on Safety And Security In Cyberspace, Tokyo, May 2001.

[1057] The experts expressed their concerns regarding implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible"; Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace, Tokyo, May 2001.

[1058] G8 Justice and Home Affairs Communiqué, Washington DC, 11 May 2004.

[1059] G8 Justice and Home Affairs Communiqué Washington DC, 11 May 2004:10. "Continuing to Strengthen Domestic Laws: To truly build global capacities to combat terrorist and criminal uses of the Internet, all countries must continue to improve laws that criminalize misuses of computer networks and that allow for faster cooperation on Internet-related investigations. With the Council of Europe Convention on Cybercrime coming into force on July 1, 2004, we should take steps to encourage the adoption of the legal standards it contains on a broad basis."

[1060] The participants expressed their intention to strengthen the instruments in the fight against cybercrime: "We discussed the necessity of improving effective countermeasures that will prevent IT terrorism and terrorist acts in this sphere of high technologies. For that, it is necessary to devise a set of measures to prevent such possible criminal acts, including in the sphere of telecommunication. That includes work against the selling of private data, counterfeit information and application of viruses and other harmful computer programs. We will instruct our experts to generate unified approaches to fighting cyber criminality, and we will need an international legal base for this particular work, and we will apply all of that to prevent terrorists from using computer and Internet sites for hiring new terrorists and the recruitment of other illegal actors". See: www.g7.utoronto.ca/justice/justice2006.htm.

[1061] Regarding the topic of cyberterrorism, see above: § 2.9.1. In addition, see: *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis,* Cyber-terrorism and Cybersecurity; www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeldt*, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: Prados, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 *et seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.*; OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf.

[1062] The summit declaration calls for measures in the fight against cyberterrorism: "Effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists". For more information, see: http://en.g8russia.ru/docs/17.html.

[1063] For more information, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1064] Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 6, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

[1065] Final Declaration of the 2009 G8 ministerial meeting of Justice and Home Affairs, Rome, page 7, available at: www.g8italia2009.it/static/G8_Allegato/declaration1giu2009,0.pdf.

[1066] G8 Summit 2010 Muskoka Declaration, 2010, available at: www.g7.utoronto.ca/summit/2010muskoka/communique.html.

[1067] See press release from 30.5.2011, available at: www.eg8forum.com/en/documents/news/Final_press_release_May_30th.pdf.

[1068] See G8 Declaration, Renewed Commitment for Freedom and Democracy, available at: www.g20-g8.com/g8-g20/g8/english/live/news/renewed-commitment-for-freedom-and-democracy.1314.html.

[1069] The United Nations (UN) is an international organization founded in 1945. It had 192 Member States in 2010.

[1070] A/RES/44/25, adopted by the UN General Assembly on 12 December 1989.

[1071] A/RES/45/121, adopted by the UN General Assembly on 14 December 1990. The full text of the resolution is available at: www.un.org/documents/ga/res/45/a45r121.htm.

[1072] UN Manual on the Prevention and Control of Computer-Related Crime (United Nations publication, Sales No. E.94.IV.5), available at www.uncjin.org/Documents/EighthCongress.html.

[1073] See the preface to the Optional Protocol.

[1074] See Art. 2.

[1075] See especially the background paper: Crimes related to computer networks, A/CONF.187/10.

[1076] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 165, available at: www.uncjin.org/Documents/congr10/15e.pdf.

[1077] Report of the tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 2000, A/CONF.185/15, No. 174, available at: www.uncjin.org/Documents/congr10/15e.pdf.

[1078] "The United Nations should take further action with regard to the provision of technical cooperation and assistance concerning crime related to computer networks".

[1079] A/RES/55/63. The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

[1080] A/RES/56/121. The full text of the resolution is available at: http://daccessdds.un.org/doc/UNDOC/GEN/N01/482/04/PDF/N0148204.pdf.

[1081] A/RES/57/239, on Creation of a global culture of cybersecurity; A/RES/58/199, on Creation of a global culture of cybersecurity and the protection of critical information infrastructure.

[1082] Measures to Combat Computer-related Crime, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, A/CONF.203/14.

[1083] Committee II Report, eleventh UN Congress on Crime Prevention and Criminal Justice, 2005, BKK/CP/19.

[1084] Report of the Western Asian Regional Preparatory Meeting for the Eleventh United Nations Congress on Crime Prevention and Criminal Justice, A/CONF.2003/RPM.4/1, No. 14.

[1085] 30(d): "Considering the feasibility of negotiation of an international instrument on preventing and combating crimes involving information technologies", see: Discussion guide to the eleventh United Nations Congress on Crime Prevention and Criminal Justice, 2003, A/CONF.203/RM.1.

[1086] Declaration Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, available at: www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

[1087] See in this context especially the background paper prepared by the secretariat.

[1088] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

[1089] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1090] „The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1091] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1092] *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

[1093] Regarding the focus of the debate, see: Recent developments in the use of science and technology by offenders and by competent authorities in fighting crime, including the case of cybercrime, twelfth UN Congress on Crime Prevention and Criminal Justice, A/CONF.213/9.

[1094] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress on Crime Prevention and Criminal Justice, Information Documents SG/Inf(2010)4, 16.02.2010, page 17 *et seq.*

[1095] Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[1096] Resolutions 55/63 and 56/121.

[1097] Resolutions 57/239 and 58/199.

[1098] Report on the meeting of the open-ended intergovernmental expert group to conduct a comprehensive studay of the problem of cybercrime held in Vienna from 17 to 21 January 2011, UNODC/CCPCJ/EG.4/2011/3.

[1099] Draft topics for consideration in a comprehensive study on the impact o fand response to cybercrime, 2010, UNODC, UNODC/CCPCJ/EG.4/2011/2.

[1100] www.unodc.org/cybercrime-study/

[1101] UNODC Press Release (26.01.2012) available at: www.unodc.org/unodc/en/frontpage/2012/January/unodc-chief-announces-a-comprehensive-study-on-cybercrime.html

[1102] United Nations Commission on Crime Prevention and Criminal Justice.

[1103] www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[1104] Vgl. Comprehensive Study on Cybercrime, UNODC, 2013, page X.

[1105] Vgl. Comprehensive Study on Cybercrime, UNODC, 2013, S. XIX.

[1106] UNODC/CCPCJ/EG.4/2013/3.

[1107] Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

[1108] Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

[1109] Commission on Crime Prevention and Criminal Justice, Report on the twenty-thrid session (13 December 2013 and 12 to 16 May 2014), Economic and Social Council, Official Records,2014, Supplement No. 10.

[1110] Commission on Crime Prevention and Criminal Justice, Report on the twenty-second session (7 December 2012 and 22 to 26 May 2013), Economic and Social Council, E/CN.15/2013/27.

[1111] Development in the Field of Information and Telecommunications in the Context of International Security, 2013, available at: www.un.org/disarmament/topics/informationsecurity/

[1112] See: Development in the Field of Information and Telecommunications in the Context of International Security, 2013, page 1.

[1113] The report on the meeting of the open-ended working group (UNODC/CCPCJ/EG.4/2011/3) is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_3/UNODC_CCPCJ_EG4_2011_3_E.pdf.

[1114] Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime, UNODC/CCPCJ/EG.4/2011/2. The document is available at: www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf.

[1115] The Commission on Crime Prevention and Criminal Justice (CCPCJ) was set up in 1991. It is a subsidiary body of the Economic and Social Council.

[1116] CCPCJ Resolution 16/2, on Effective crime prevention and criminal justice responses to combat sexual exploitation of children. Regarding the discussion process in the development of the resolution and for an overview of different existing legal instruments, see: Note by the Secretariat regarding Commission on Crime prevention and criminal justice responses to urban crime, including gang-related activities, and effective crime prevention and criminal justice responses to combat sexual exploitation of children, CN.15/2007/CRP.3, available at: www.unodc.org/pdf/crime/session16th/E_CN15_2007_CRP3_E.pdf. Regarding the initiative relating to the resolution, see: www.america.gov/st/washfile-english/2007/April/20070423135940ajesrom0.709469.html.

[1117] The United Nations Economic and Social Council (ECOSOC) is a principal organ to coordinate economic, social, and related work and serve as a central forum for discussing international economic and social issues. For more information, see: www.un.org/ecosoc/.

[1118] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-26.pdf.

[1119] For more information on the development process and the work of the intergovernmental expert group, see: Results of the second meeting of the Intergovernmental Expert Group to Prepare a study on Fraud and the Criminal Misuse and Falsification of Identity, Commission on Crime Prevention and Criminal Justice, 16th session, 2007, E/CN.15/2007/8, page 2.

[1120] ECOSOC Resolution 2007/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime, available at: www.un.org/ecosoc/docs/2007/Resolution%202007-20.pdf.

[1121] Regarding Internet-related ID-theft, see above: § 2.8.3, and below: § 6.2.16.

[1122] ECOSOC Resolution 2004/26, on International cooperation in the prevention, investigation, prosecution and punishment of fraud, the criminal misuse and falsification of identity and related crimes.

[1123] ECOSOC Resolution 2004/20, on International cooperation in the prevention, investigation, prosecution and punishment of economic fraud and identity-related crime.

[1124] Reports related to the activities of the working group are published. See: First meeting of the Core Group of Experts on Identity-Related Crime, Courmayeur Mont Blanc, Italy, 29-30 November 2007, available at: www.unodc.org/documents/organized-crime/Courmayeur_report.pdf (last visited: October 2008); Second meeting of the Core Group of Experts on Identity-Related Crime, Vienna, Austria, 2-3 June 2008, available at: www.unodc.org/documents/organized-crime/Final_Report_ID_C.pdf (last visited: October 2008).

[1125] See for example: Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, 2009, E/CN.15/2009/CRP.13.

[1126] ECOSOC Resolution 2004/42, on Sale of internationally controlled licit drugs to individuals via the Internet, available at: www.un.org/ecosoc/docs/2004/Resolution%202004-42.pdf.

[1127] For further information see: www.unodc.org/unodc/en/frontpage/2011/May/unodc-and-itu-to-cooperate-more-closely-to-make-the-internet-safer.html.

[1128] The International Telecommunication Union (ITU) with headquarters in Geneva was founded as the International Telegraph Union in 1865. It is a specialized agency of the United Nations. ITU has 192 Member States and more than 700 Sector Members and Associates. For more information, see: www.itu.int.

[1129] WSIS Geneva Plan of Action, 2003, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1160|0.

[1130] WSIS Tunis Agenda for the Information Society, 2005, available at: www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=2267|0.

[1131] For more information on Action Line C5, see: http://www.itu.int/wsis/c5/, and also the meeting report of the second Facilitation Meeting for WSIS Action Line C5, 2007, page 1, available at: www.itu.int/osg/csd/cybersecurity/pgc/2007/events/docs/meetingreport.pdf and the meeting report of the third Facilitation Meeting for WSIS Action Line C5, 2008, available at: www.itu.int/osg/csd/cybersecurity/WSIS/3rd_meeting_docs/WSIS_Action_Line_C5_Meeting_Report_June_2008.pdf.

[1132] For more information, see www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1133] www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1134] The five pillars are: legal measures, technical and procedural measures, organizational structures, capacity building, international cooperation. For more information, see: www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.

[1135] See: www.itu.int/osg/csd/cybersecurity/gca/hleg/index.html.

[1136] www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; See: *Gercke*, Zeitschrift fuer Urheber- und Medienrecht, 2009, Issue 7, page 533.

[1137] See, in this context: *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1, page 7 *et seq*.

[1138] Global Strategic Report, Chapter 1.6.

[1139] Global Strategic Report, Chapter 1.7.

[1140] Global Strategic Report, Chapter 1.10.

[1141] Global Strategic Report, Chapter 1.11.

[1142] 23-25 November 2009 (Santo Domingo, Dominican Republic): www.itu.int/ITU-D/cyb/events/2009/santo-domingo; 23-25 September 2009 (Hyderabad, India): 2009 ITU Regional Cybersecurity Forum for Asia-Pacific; 4-5 June 2009 (Tunis, Tunisia): 2009 ITU Regional Cybersecurity Forum for Africa and Arab States; 18-22 May 2009 (Geneva, Switzerland): WSIS Forum of Events 2009, including Action Line C5 dedicated to building confidence and security in the use of ICTs, and activities for child online protection; 7-9 September 2009 and 6-7 April 2009 (Geneva, Switzerland): ITU-D Rapporteur's Group Meeting on Question 22/1 on Securing Information and Communication Networks; 7-9 October 2008 (Sofia, Bulgaria): ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS); 25-28 August 2008 (Lusaka, Zambia): ITU Regional Cybersecurity Forum for Eastern and Western Africa; 15-18 July 2008 (Brisbane, Australia): ITU Regional Cybersecurity Forum for Asia Pacific and Seminar on the Economics of Cybersecurity; 18-21 February 2008 (Doha, Qatar): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP) and Cybersecurity Forensics Workshop; 27-29 November 2007 (Praia, Cape Verde): ITU West Africa Workshop on Policy and Regulatory Frameworks for Cybersecurity and CIIP, 29-31 October 2007 (Damascus, Syria): ITU Regional Workshop on E-Signatures and Identity Management; 16-18 October 2007 (Buenos Aires, Argentina): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP); 17 September 2007 (Geneva, Switzerland): Workshop on Frameworks for National Action: Cybersecurity and Critical Information Infrastructure Protection (CIIP); 28-31 August 2007 (Hanoi, Vietnam): ITU Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection (CIIP).

[1143] Details about the project and the funding are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/.

[1144] For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html; ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 4.

[1145] Information about the project are available at: www.itu.int/ITU-D/treg/projects/itu-ec/index.html.

[1146] The adoption took place during the 3rd Ordinary General Assembly oft he West African Telecommunications Regulators Assembly.

[1147] www.itu.int/ITU-D/treg/projects/itu-ec/ECOWAS_MINISTERS_ADOPTS_GUIDELINES_FOR_TELECOMMUNICATION_MARKET_AT_ABUJA.pdf

[1148] http://news.ecowas.int/en/presseshow.php?nb=2&lang=en&annee=2007

[1149] Angla, Benin, Botswana, Burkina Faso, Burundi, Cameroon, Cap-Verde, Chad, Congo, Cote d'Ivoire, Eritrea, Gabon, Gambia, Ghana, Guinea, Guinea Equatorial, Guinea-Bissau, Kenya, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritius, Mozambique, Namibia, Niger, Nigeria, Uganda, Central African Republic, Democratic Republic of Congo, Rwanda, Sao Tome-e-Principe, Senegal, Seychelles, Sierra Leone, South Africa, Swaziland, Tanzania, Togo, Zambia and Zimbabwe.

[1150] ACP-EU Joint Parliamentary Assembly, Committee on Economic Development, Finance and Trade, Draft Report on ICT-based entrepreneurship and its impact on development in ACP countries, 2012, page 5.

[1151] The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

[1152] CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

[1153] Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

[1154] Detailed information about requested support, activities and documents are available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/

[1155] For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[1156] Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

[1157] The Council of Europe, based in Strasbourg and founded in 1949, is an international organization representing 47 Member States in the European region. The Council of Europe is not to be confused with the Council of the European Union and the European Council (informally called the European Summit), as the Council of Europe is not part of the European Union, but a separate organization. In the first edition of this guide, the Council of Europe Convention was

listed as an international approach. In consistency with the status of the international debate and UNGA Resolution 60/177, it is characterized as a regional approach and has been moved to this section.

[1158] Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime in Strasbourg, 1976.

[1159] The Expert Committee consisted of 15 experts, as well as observers from Canada, Japan, United States, the EEC, OECD and UN. Source: *Nilsson* in *Sieber*, Information Technology Crime, page 577.

[1160] United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1161] *Nilsson* in Sieber, Information Technology Crime, page 576.

[1162] Recommendation No. R (89) 9, adopted by the Committee of Ministers on 13 September 1989 at the 428th Meeting of the Ministers Deputies.

[1163] Recommendation No. R (95) 13, adopted by the Committee of Ministers on 11 September 1995 at the 543rd Meeting of the Ministers Deputies.

[1164] The Guidelines deal with investigative instruments (e.g. search and seizure) as well as electronic evidence and international cooperation.

[1165] Decision CDPC/103/211196. CDPC explained its decision by pointing out the international dimension of computer crimes: "By connecting to communication and information services, users create a kind of common space, called "cyber-space", which is used for legitimate purposes, but may also be the subject of misuse. These "cyber-space offences" are either committed against the integrity, availability and confidentiality of computer systems and telecommunication networks or they consist of the use of such networks of their services to commit traditional offences. The transborder character of such offences, e.g. when committed through the Internet, is in conflict with the territoriality of national law enforcement authorities."

[1166] Explanatory Report of the Convention on Cybercrime (185), No. 10.

[1167] The full text of Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: www.coe.int.

[1168] For more details about the offences covered by the Convention, see below: § 6.2.; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*,
The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cyber-crime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No.4, 2001, page 889 *et seq.*

[1169] Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

[1170] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Iceland, Italy, Latvia, Lithuania, Malta, Moldova, Montenegro, Netherlands, Norway, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, United States.

[1171] The need for a ratification is laid down in Article 36 of the Convention on Cybercrime:

Article 36 – Signature and entry into force

1) This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.

2)This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

1172 Australia, Dominican Republic, Mauritius and Philippines.

1173 Argentina, Australia, Chile, Colombia, Costa Rica, Dominican Republic, Israel, Mauritius, Mecixo, Panama, Philippines, Senegal.

1174 Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico and Philippines.

1175 Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention on Cybercrime shall be distributed to all Interpol member countries in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp; The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf; APEC called for economies to study the Convention on Cybercrime, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html; OAS called for an evaluation of the Convention while designing Cybercrime legislation, see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 19, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html

1176 Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

1177 Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime No. 4: "The committee drafting the Convention on Cybercrime discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention on Cybercrime."

1178 Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; Baker; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

1179 United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 234, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1180 See Art. 3 of the Fourth Draft Convention, PC-CY (98) Draft No. 4, 17.04.1998.

1181 Albania, Armenia, Austria, Belgium, Bosnia and Herzegovina, Canada, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovenia, Sweden, Switzerland, South Africa, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine.

1182 Albania, Armenia, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Finland, France, Germany, Latvia, Lithuania, Montenegro, Netherlands, Norway, Portugal, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine.

1183 Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries

shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp. The 2005 WSIS Tunis Agenda states: "We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiatives including, but not limited to, the Council of Europe's Convention on Cybercrime", available at: http://ec.europa.eu/information_society/activities/internationalrel/docs/wsis/tunis_agenda.pdf.

[1184] For more information on the achievements and shortcomings see: *Gercke*, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

[1185] Draft Code of Criminal Procedure, written by the Advisory Committee on the Reform of Criminal Procedural Legislation, set up by Decree No. 115 of the National Executive Power of 13 February 2007 (Boletín Oficial of 16 February 2007).

[1186] Draft Electronic Crime Act 2006.

[1187] Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefore and for other Purposes, House Bill No. 3777.

[1188] Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[1189] Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

[1190] Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

[1191] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, page 18.

[1192] Argentina, Australia, Chile, Costa Rica, Dominican Republic, Mexico, Philippines and Senegal.

[1193] Albania, Croatia,

[1194] Estonia, Hungary.

[1195] Lithuania, Romania, Slovenia, The former Yugoslav Republic of Macedonia.

[1196] Bulgaria, Cyprus, Denmark.

[1197] Armenia, Bosnia and Herzegovina, France, Netherlands, Norway, Ukraine, United States.

[1198] Finland, Iceland, Latvia.

[1199] Italy, Slovakia.

[1200] Germany, Moldova, Serbia.

[1201] Azerbaijan, Montenegro, Portugal, Spain.

[1202] United Kingdom, Switzerland.

[1203] Austria, Belgium, Georgia, Malta, Australia and Japan.

[1204] Czech Republic, Dominican Republic and Mauritius.

[1205] See Sec. 202a of the German Penal Code.

[1206] Country profiles can be downloaded at www.coe.int/cybercrime.

[1207] For details on the requirements, see: *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025, available at: www.fas.org/sgp/crs/misc/97-1025.pdf.

[1208] *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1209] See in this context, for example: *OECD*, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, 2005, page 4,

[1210] See Art. 44 Convention on Cybercrime.

1211 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

1212 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1213 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

1214 "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

1215 *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009.

1216 Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

1217 See *Gercke*, How Terrorist Use the Internet in *Pieth/Thelesklaf/Ivory*, Countering Terrorist Financing, 2009, page 127-150.

1218 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

1219 The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions. See *Gercke*, Criminal Responsibility for Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.8.4. Regarding the legal response to phishing, see: *Lynch*, Identity Theft in Cyberspace: Crime Control, Berkeley Tech. Law Journal, 2005, 259; *Hoffhagle*, Identity Theft: Making the Known Unknowns Known, Harvard Journal of Law & Technology, Vol. 21, No. 1, 2007, page 97 *et seq.*

1220 Criticism about the lack of coverage of such topics in the existing instruments: *Vogel*, Towards a Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP / e-RIAPL, 2008, C-07, page 7.

1221 See: Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, COM(2010) 517, page 6.

1222 *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007, page 28, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

1223 See Art. 44 Convention on Cybercrime.

1224 See Art. 37 Convention on Cybercrime.

1225 "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations No. 41 (page 10).

1226 "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations No. 47 (page 10).

[1227] "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations No. 29 (page 7).

[1228] "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations No. 40 (page 10).

[1229] See: Development Gateway's Special Report, Information Society – Next Steps?, 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[1230] See: Art. 41 Salvador Declaration on Comprehensive Strategies for Global Challenges, 2010. Available at: www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/Salvador_Declaration/Salvador_Declaration_E.pdf.

[1231] See ITU Resolution 130 (Rev. Guadalajara, 2010).

[1232] Andorra, Monaco and San Marino did not even sign the Convention. Lichtenstein and Malta signed but never ratified the Convention.

[1233] See Explanatory Report to the Convention on Cybercrime, No. 298.

[1234] *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf

[1235] The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

[1236] ICB4PAC Workshop on Concepts and Techniques of Developing CyberCrime Policy and Legislation, Apia, Samoa 22-25 August 2011.

[1237] Contribution of the Secretary General of the Council of Europe to the twelfth United Nations Congress, ID SG/Inf(2010)4, 2010, No. 47.

[1238] Model Law on Computer and Computer Related Crime, LMM(02)17. For more information about the Model Law see:

[1239] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

[1240] For further information and references on electronic evidence see blow: § 6.5.

[1241] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[1242] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1243] Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Ireland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia and Turkey. Albania, Armenia, Azerbaijan, Denmark, Estonia, Georgia, Hungary, Iceland, Italy, Liechtenstein, Luxembourg, Malta, Monaco, Montenegro, Slovakia, Spain, Switzerland, Ukraine and the United Kingdom followed.

[1244] Albania Austria, Bosnia and Herzegovina, Bulgaria, Croatia, Denmark, Finland, France, Greece, Luxembourg, Malta, Montenegro, Netherlands, Romania, San Marino, Serbia, Spain and Turkey.

[1245] For more details, see: *Gercke*, The Development of Cybercrime Law, Zeitschrift fuer Urheber- und Medienrecht 2008, 550ff.

[1246] Cybercrime Convention Committee (T-CY)

[1247] Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3.

[1248] Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3, p. 58.

[1249] Transborder Access and Jurisdiction: What are the options?, 2012, T-CY (2012) 3, p. 58.

[1250] EDRI, Transborder Data Access: Strong Criticsm on planst o extend CoE Cybercrime Treaty, 5.6.2013, available at: www.edri.org/edrigram/number11.11/transborder-data-access-cybercrime-treaty.

[1251] Report of the Transborder Group for 2013, Cybercrime Convention Committee, T-CY (2013) 30.

[1252] 1: transborder access with consent but without the limitation to data stored “in another Party”; 2: transborder access without consent but with lawfully obtained credentials; 3: transborder access without consent in good faith or in exigent or other circumstances; 4: extending a search from the original computer to connected systems without the limitation “in its territory”; 5: the power of disposal as connecting legal factor.

[1253] T-CY Guidance Note #3 Transborder Access to Data (Article 32), Cybercrime Convention Committee, T-CY (2013) 7E.

[1254] The European Union is a supranational and intergovernmental union with, as at today, 27 Member States from the European continent.

[1255] One example is the EU funded HIPCAR project on Enhancing Competitiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures. For more information, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1256] *Herlin-Karnell*, Commission v. Council: Some reflections on criminal law in the first pillar, European Public Law, 2007, page 69 *et seq.*; *Herlin-Karnell,* Recent developments in the area of European criminal law, Maastricht Journal of European and Comparative Law, 2007, page 15 *et seq.*; *Ambos*, Is the development of a common substantive criminal law for Europe possible? Some preliminary reflections, Maastricht Journal of European and Comparative Law, 2005, 173 *et seq.*

[1257] See: *Satzger*, International and European Criminal Law, 2005, page 84 for further reference.

[1258] itle VI, Treaty on European Union.

[1259] Framework Decision 2003/80/JHI, OJ L 29, 5.2.2003.

[1260] Decision of the Court of Justice of the European Communities, 13.09.2005, Case C-176/03. See in this context: *Gercke.*

[1261] Communication from the Commission to the European Parliament and the Council on the implications of the Court’s judgement of 13 September 2005 (Case C-176/03 Commission v Council), 24.11.2005, COM(2005) 583.

[1262] Decision of the Court of Justice of the European Communities, 23.10.2007, Case C-440/05; See in this context: *Eisele*, Anmerkung zum Urteil des EuGH C 440/05, JZ 2008, page 251 *et seq.*; *Fromm*, Anmerkung zum Urteil des EuGH C 440/05, ZIS 2008, page 168 *et seq.*

[1263] ABl. 2007 C 306, 1.

[1264] Regarding the impact of the reform on the harmonization of criminal law, see: *Peers*, EU criminal law and the Treaty of Lisbon, European law review 2008, page 507 *et seq.*; *Zeder*, EU-minimum rules in substantive penal law: What will be new with the Lisbon Treaty?, ERA Forum 2008, page 209 *et seq.*

[1265] Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009.

[1266] Regarding the Hague Programme, see: *Braum*, Das Haager-Programm der Europaeischen Union: falsche und richtige Schwerpunkte europaeischer Strafrechtsentwicklung in *Joerden/Szwarc*, Europaeisierung des Strafrechts in Deutschland und Polen, 2007, page 11 *et seq.*

[1267] See: Stockholm Programme, An open and secure Europe serving and protecting the citizens, 2009, No. 3.3.1.

[1268] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

[1269] See: Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487, page 24.

[1270] Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

[1271] Communication of 8 December 1999 on a Commission initiative for The Lisbon Special European Council, 23 and 24 March 2000 – *e*Europe – An information society for all – COM 1999, 687. See in this regard also: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

[1272] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions – Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, 26.1.2001, COM(2000) 890.

[1273] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

[1274] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM(2000) 890, page 23.

[1275] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 31.

[1276] Communication From The Commission To The Council, The European Parliament, The Economic And Social Committee And The Committee Of The Regions Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, page 32.

[1277] Network and Information Security – A European Policy approach – adopted 6 June 2001.

[1278] For example the Council in 1999, available at: http://db.consilium.eu.int/de/Info/eurocouncil/index.htm.

[1279] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime, COM (2007) 267. For more information see: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 17, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1280] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union E-Commerce Regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*

[1281] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

[1282] See Directive 2000/31/EC, recital 1 *et seq.*

[1283] For more details, see below: § 6.

[1284] *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010, page 75 *et seq.*

[1285] Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions – Illegal and harmful content on the Internet. COM (1996) 487.

[1286] Decision No. 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks (276/1999/EC).

[1287] Council Framework Decision of 28 May 2001 on combating fraud and counterfeiting of non-cash means of payment (2001/413/JHA).

[1288] See Art. 4 of the Framework Decision.

[1289] This instrument was in the meantime substituted by the 2012 Directive (see below).

[1290] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The legal basis for the Framework Decision, indicated in the preamble of the proposal for the Framework Decision is Articles 29, 30(a), 31 and 34(2)(b) of the Treaty on European Union. See: *Gercke*, Framework Decision on Attacks against Information

Systems, CR 2005, 468 *et seq.*; *Sensburg*, Schutz vor Angriffen auf Informationssystem: Weiterer Schritt zum europaeischen Strafrecht?, Kriminalistik 2007, page 607ff.

1291 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1292 See the explanation of the Framework Decision in the Proposal For A Council Framework Decision on combating serious attacks against information systems, No. 1.6.

1293 Council Framework Decision 2005/222/JHA of 24.02.2005 on attacks against information systems, recital 5.

1294 Directive of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communication networks and amending directive 2002/58/EC. Document 2005/0182/COD.

1295 See below.

1296 *Gercke*, The Development of Cybercrime Law in 2005, Zeitschrift fuer Urheber- und Medienrecht 2006, page 286.

1297 European Court of Justice, Case C-275/06.

1298 See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

1299 In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

1300 Data Retention Directive, recital 6.

1301 Data Retention Directive, recital 6.

1302 Case C-301/06.

1303 Judgement in Joined Cases C-293/12 and C-594/12.

1304 Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

1305 "Article 4 of the Framework Decision on combating terrorism states that inciting, aiding or abetting terrorist offences should be made punishable by the Member States. Article 2 of the same instrument requires Member States to hold those directing a terrorist group or participating in its activities criminally liable. However, these provisions do not explicitly cover the dissemination of terrorist propaganda and terrorist expertise, in particular through the Internet."

1306 "Training for terrorism" means to provide instruction in the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods or techniques, for the purpose of committing one of the acts listed in Article 1(1), knowing that the skills provided are intended to be used for this purpose.

1307 Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, COM (2010) 94.

1308 Directive 2011/92/EU of the European Parliament and of The Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

1309 See: Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA, page 2.

1310 ETS 201. For more information see: § 5.2.1

1311 See Art. 5, No. 3, of the Draft Directive.

1312 Regarding the challenges related to the use of encryption technology, see above: § 3.2.13. One survey on child pornography suggested that only 6 per cent of arrested child pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: http://www.missingkids.com/en_US/publications/NC144.pdf.

1313 See Explanatory Report to the Convention on the Protection of Children, No. 140.

[1314] The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180.

[1315] Regarding the underlying technology, see: *Austerberrry*, The Technology of Video & Audio Streaming, 2004, page 130 *et seq.*; *Wu/Hou/Zhu/Zhang/Peha*, Streaming Video over the Internet: Approaches and Directions, IEEE Transactions on Circuits and Systems for Video Technology, Vol. 11, No. 3, 2001, page 282 *et seq.*; *Garfia/Pau/Rico/Gerla*, P2P Streaming Systems: A Survey and Experiments, 2008.

[1316] Regarding filter obligations/approaches, see*: Lonardo*, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 *et seq.*; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Edwards/Griffith*, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Research Service, Nov. 2008; *Zittrain/Edelman*, Documentation of Internet Filtering Worldwide.

[1317] See *Gercke*, The Role of Internet Service Providers in the Fight against Child Pornography, Computer Law Review International, 2009, page 69 *et seq.*

[1318] *Clayton/Murdoch/Watson*, Ignoring the Great Firewall of China, available at: www.cl.cam.ac.uk/~rnc1/ignoring.pdf; *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 53; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

[1319] *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page 73.

[1320] *Sieber/Nolde*, Sperrverfuegungen im Internet, 2008, page 55.

[1321] *Pfitzmann/Koepsell/Kriegelstein*, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf.

[1322] *Callanan/Gercke/De Marco/Dries-Ziekenheiner*, Internet Blocking – Balancing Cybercrime Responses in Democratic Societies, 2009, page 131 *et seq.*; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008, page ix.

[1323] Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.

[1324] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Deciion 2005/222/JHA.

[1325] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1326] Proposal for a Directive of the European Parliament and the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, page 3.

[1327] 1999/364/JHA: Common Position of 27 May 1999 adopted by the Council on the basis of Article 34 of the Treaty on European Union, on negotiations relating to the draft Convention on Cyber Crime held in the Council of Europe.

[1328] See Art. 1 of the Common Position.

[1329] See in this context: *Buono*, Investigating and prosecuting crimes in cyberspace, to be published in ERA Forum 2010.

[1330] See *Gercke*, The Slow Awake of a Global Approach against Cybercrime, Computer Law Review International, page 145.

[1331] The Organisation for Economic Co-operation and Development was founded 1961. It has 34 member countries and is based in Paris. For more information, see: www.oecd.org.

[1332] *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 8, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1333] OECD, Computer-related Criminality: Analysis of Legal Policy in the OECD Area, OECD, Report DSTI-ICCP 84.22 of 18 April 1986.

[1334] In 1992, the Council of the OECD adopted the Recommendation concerning Guidelines for the Security of Information Systems. The 24 OECD member countries adopted the guidelines later.

[1335] Adopted by the OECD Council at its 1037th session on 25 July 2002. The 2002 OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security, available at: www.oecd.org/document/42/0,3343,en_2649_34255_15582250_1_1_1_1,00.html.

[1336] Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1337] See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1338] The report is available at: www.legislationline.org/upload/lawreviews/6c/8b/82fbe0f348b5153338e15b446ae1.pdf.

[1339] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

[1340] Scoping Paper on Online Identity Theft, Ministerial Background Report, DSTI/CP(2007)3/FINAL, 2008, page 5, available at: www.oecd.org/dataoecd/35/24/40644196.pdf.

[1341] Computer Viruses and other malicious software: A threat to the internet economy, OECD, 2009.

[1342] The Asia-Pacific Economic Cooperation (APEC) is a group of Pacific Rim countries dealing with the improvement of economic and political ties. It has 21 members.

[1343] "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

[1344] The Ministers stated in the declaration "their call for continued collaboration and sharing of information and experience between member economies to support a safe and trusted ICT environment including effective responses to ensure security against cyber threats, malicious attacks and spam." For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html.

[1345] Australia, Brunei Darussalam, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Philippines, Singapore, Chinese Taipei, Thailand and United States.

[1346] See: Report to Leaders and Ministers on Actions of the Telecommunications and Information Working Group to Address Cybercrime and Cybersecurity, 2003/AMM/017.

[1347] APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, on 26 October 2002. Regarding national legislation on cybercrime in the Asian-Pacific region, see: *Urbas*, Cybercrime Legislation in the Asia-Pacific Region, 2001, available at: www.aic.gov.au/conferences/other/urbas_gregor/2001-04-cybercrime.pdf. See also in this regard: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 18, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1348] APEC TEL-OECD Malware Workshop (2007); APEC TEL and ASEAN Workshop on Network Security (2007); Workshop on Cyber Security and Critical Information Infrastructure Protection (CIIP); APEC Symposium on Spam and Related Threats (2007); APEC Best Practices In International Investigations Training Sessions (2004); Conference on cybercrime for the APEC region (2005); Conference on cybercrime for the APEC region (2004); Conference on cybercrime for the APEC region (2003); Cybercrime legislation training workshops (several, 2003); Judge and Prosecutor Capacity Building Project.

[1349] "We also call for closer cooperation between law enforcement officials and businesses in the field of information security and fighting computer crime." APEC Leaders' Statement On Fighting Terrorism And Promoting Growth, Los Cabos, Mexico, 26 October 2002.

[1350] Cybercrime Legislation and Enforcement Capacity Building Project – 3rd Conference of Experts and Training Seminar, APEC Telecommunications and Information Working Group, 32nd Meeting, 5-9 September 2005, Seoul, Korea.

[1351] "Economies are currently implementing and enacting cybersecurity laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project will support institutions to implement new laws."

[1352] The APEC Telecommunications and Information Working Group was founded in 1990. It aims to improve telecommunications and information infrastructure in the Asia-Pacific region by developing information policies. For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[1353] For more information, see: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.MediaLibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/som/mtg/2002/word.Par.0204.File.v1.1

[1354] See: www.apec.org/apec/apec_groups/som_committee_on_economic/working_groups/telecommunications_and_information.html

[1355] Cybercrime Legislation & Enforcement Capacity Building Workshop, and Electronic Commerce Steering Group Meeting.

[1356] 2003/SOMIII/ECSG/O21.

[1357] *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf.

[1358] See: Model Law on Computer and Computer Related Crime, LMM(02)17, Background information.

[1359] See: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf (Annex 1).

[1360] Model Law on Computer and Computer Related Crime, LMM(02)17; the Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1361] Draft Model Law on Electronic Evidence, LMM(02)12.

[1362] For more information see: www.waigf.org/IMG/pdf/Cybercrime_Initiative_Outline.pdf.

[1363] For more information see: African Union, Oliver Tambo Declaration, Johannesburg 2009, available at: www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf.

[1364] The Draft Convention is available for download at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf

[1365] See Part 1, Sec. II, Ch. II.

[1366] See Part 1, Sec. IV.

[1367] See Part 1, Sec. V.

[1368] See Part 2.

[1369] Art. III-1.

[1370] Part 3, Chaptr 1, Art. 1 and Art. 2.

[1371] Art. III-1-1 to Art. III-1-7

[1372] Art. III-1-8 to Art. III-1-12.

[1373] Art. III-2.

[1374] Art. III-3.

[1375] Art. III-4.

[1376] Art. III-5.

[1377] Art. III-6.

[1378] Art. III-7 1).

[1379] For more information see below: § 6.2.2.

[1380] Art. III-8.

[1381] Art. III-9.

[1382] Art. III-10.

[1383] Art. III-11.

[1384] Art. III-12.

[1385] Art. III-13.

[1386] Art. III-14.

[1387] Art. III-15.

[1388] Art. III-16.

[1389] Art. III-17.

[1390] Art. III-19.

[1391] Art. III-20.

[1392] Art. III-21.

[1393] Art. III-22.

[1394] Art. III-24.

[1395] Art. III-25.

[1396] Art. III-26.

[1397] Art. III-27.

[1398] Art. III-36.

[1399] Art. III-37.

[1400] Art. III-39.

[1401] Art. III-41.

[1402] Regarding reasons for this delay see for example: Gareth van Zyl, Adoption of flawed AU cybersecurity convention postponed, IT Web Africa, 21.01.2014, available at: www.itwebafrica.com/ict-and-governance/523-africa/232273-adoption-of-flawed-au-cybersecurity-convention-postponed.

[1403] The League of Arab States is a regional organization, with currently 22 members.

[1404] See: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 20, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1405] Draft Electronic Crime Act 2006.

[1406] Draft Law on Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[1407] Law No. 2 of 2006, enacted in February 2006.

[1408] Regional Conference Booklet on: Cybercrime, Morocco, 2007, page 6, available at: www.pogar.org/publications/ruleoflaw/cybercrime-09e.pdf.

[1409] Decision of the Arab Justice Ministers Council, 19th session, 495-D19-8/10/2003.

[1410] Bahrain, Kuwait, Oman, Qatar, Saudi Arabia and UAE.

[1411] Non-official translation of the recommendations of the Conference on Combating Cybercrime in the GCC Countries, 18 June 2007, Abu Dhabi:

1) Calling for the adoption of a treaty by the Gulf Cooperation Council (GCC) countries, inspired by the Council of Europe Cybercrime convention, to be expanded later to all Arab countries.

2) Calling all GCC countries to adopt laws combating cybercrime inspired by the model of the UAE cybercrime Law.

3) Calling for the adoption of laws in relation to procedural matters such as seizure, inspection and other investigation procedures for such special type of crimes.

5) Providing trainings to inspection and law enforcement officials on dealing with such crimes.

6) Providing sufficient number of experts highly qualified in new technologies and cybercrime particularly in regard to proof and collecting evidence.

7) Recourse to the Council of Europe's expertise in regard to combating cybercrime particularly in regard to studies and other services which would contribute in the elaboration and development of local countries legislation in GCC countries.

8) Harmonization of the legislations in Arab and particularly GCC countries in regard to basic principles in combating this type of crimes on both procedural and substantive level.

9) Increasing cooperation between public and private sectors in the intent of raising awareness and exchange of information in the cybercrime combating field.

1412 The Organization of American States is an international organization with 34 active Member States. For more information, see: www.oas.org/documents/eng/memberstates.asp.

1413 For more information, see: www.oas.org/juridico/english/cyber.htm, and the Final report of the Fifth Meeting of REMJA, which contains the full list of reports, results of the plenary session and conclusions and recommendations, at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

1414 The conclusions and recommendation of the meetings of Ministers of Justice or of Ministers or Attorneys General of the Americas on Cyber Crime are available at: www.oas.org/juridico/english/cyber_meet.htm.

1415 The full list of recommendations from the 2000 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_iii_meeting.htm#Cyber. The full list of recommendations from the 2003 meeting is available at: www.oas.org/juridico/english/ministry_of_justice_v.htm.

1416 The OAS General Secretariat, through the Office of Legal Cooperation of the Department of International Legal Affairs, serves as the technical secretariat to this Group of Experts, pursuant to the resolutions of the OAS General Assembly. More information on the Office of Legal Cooperation is available at: www.oas.org/dil/department_office_legal_cooperation.htm.

1417 In addition, the Working Group of Governmental Experts on cybercrime recommended that training be provided in the management of electronic evidence and that a training programme be developed to facilitate states link-up to the 24 hour/7 day emergency network established by the G8 to help conduct cybercrime investigations. Pursuant to such recommendation, three OAS regional technical workshops were held during 2006 and 2007, the first being offered by Brazil and the United States, and the second and third by the United States. The list of technical workshops is available at: www.oas.org/juridico/english/cyber_tech_wrkshp.htm.

1418 In the meantime, OAS has established joint collaboration with the Council of Europe and attended and participated in the 2007 Octopus Interface Conference on Cooperation against cybercrime. See: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy%20activity%20Interface2007/Interface2007_en.asp.

1419 Conclusions and Recommendations of REMJA-VII, 2008, are available at: www.oas.org/juridico/english/cybVII_CR.pdf.

1420 Conclusions and Recommendations of REMJA-VIII, 2010, are available at: www.oas.org/en/sla/dlc/remja/recom_VIII_en.pdf.

1421 The seventh meeting of the working group on Cybercrime took place from 6-7 February 2012.

1422 Recommendation of the Working Group: OEA/Ser.K/XXXIV, CIBER-VII/doc.6/12rev.1.

1423 Recommendation of the Working Group: OEA/Ser.K/ XXXIV, CIBER-VII/doc.6/12rev.1.

1424 Recommendation of the Working Group: OEA/Ser.K/ XXXIV, CIBER-VII/doc.6/12rev.1.

1425 The eighth meeting oft he Working Group on Cyber-Crime took place from 27-28 February 2014.

1426 mendation of the Working Group: OEA/Ser.K/XXXIV, CIBER-VIII/doc.4/14rev.1.

1427 For more information about the project, see: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1428 The beneficiary countries are: Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Suriname and Trinidad and Tobago.

1429 CARIFORUM is a regional organization of 15 independent countries in the Caribbean region (Antigua and Barbuda, Bahamas, Barbados, Belize, Dominica, Dominican Republic, Grenada, Guyana, Haiti, Jamaica, Saint Kitts and Nevis, Saint Lucia, Saint Vincent and the Grenadines, Suriname, and Trinidad and Tobago).

1430 Electronic transactions, Electronic evidence in e-commerce, Privacy and data protection, Interception of communications, Cybercrime, Access to public information (freedom of information), Universal access and service, Interconnection and access and finally Licensing.

1431 The assessment report is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

1432 The workshop was held in Saint Lucia on 8-12 March 2010. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1433] For further information about the project see: www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/index.html.

[1434] Cook Islands, East Timor, Fiji, Kiribati, Marshall Islands, Federated States of Micronesia, Nauru, Niue, Palau, Papua New Guinea, Samoa, Salomon Islands, Tonga, Tuvalu and Vanuatu.

[1435] More information about the event are available at: http://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/port_vila/port_vila.html.

[1436] The assessment report will be made available through the project website.

[1437] www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/events/2011/samoa/samoa.html.

[1438] More information about the event are available at: www.spc.int/en/component/content/article/704-responding-to-cybercrime-threats-in-the-pacific.html.

[1439] An overview about the output of the conference is available at: and www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy_activity_tonga_apr_11/AGREED_Cybercrime_Workshop_Outcomes.pdf.

[1440] The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_data_protection.pdf

[1441] The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_e-transactions.pdf

[1442] The model legislation that was developed with the support of ITU is available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_cybercrime.pdf

[1443] *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf.

[1444] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf ; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf. ABA International Guide to Combating Cybercrime, 2002, page 78.

[1445] Council of Europe Convention on Cybercrime (CETS No. 185), available at: http://conventions.coe.int. For more details about the offences covered by the Convention, see below: § 6.2; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; *Gercke*, The Slow Awake of a Global Approach Against Cybercrime, Computer Law Review International, 2006, 140 *et seq.*; *Gercke*, National, Regional and International Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002, No. 1, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf; *Jones*, The Council of Europe Convention on Cybercrime, Themes and Critiques, 2005, available at: www.cistp.gatech.edu/snsp/cybersecurity/materials/callieCOEconvention.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006, page 408 *et seq.*; Adoption of Convention on Cybercrime, International Journal of International Law, Vol. 95, No. 4, 2001, page 889 *et seq*.

[1446] Regarding the application of Art. 23 *et seq.* with regard to traditional crimes, see: Explanatory Report to the Convention on Cybercrime, No. 243.

[1447] *Schjolberg*, A Cyberspace Treaty – A United Nations Convention or Protocol on Cybersecurity and Cybercrime, twelfth UN Crime Congress, 2010, A/CONF.213, page 3, available at: www.cybercrimelaw.net/documents/UN_12th_Crime_Congress.pdf.

[1448] *Schjolberg/Ghernaouti-Helie*, A Global Protocol on Cybersecurity and Cybercrime, 2009, available at: www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf.

[1449] Available online: www.cybercrimelaw.net/documents/140626_Draft_Treaty_text.pdf.

[1450] For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International, 2008, page 7 *et seq.*

[1451] "The Meeting also noted the imperative need to develop an international convention on cybercrime", Report of the Latin American and Caribbean Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in San Jose from 25 to 27 May 2009, A/CONF.213/RPM.1/1, Conclusions and Recommendations, No. 41 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Western Asian Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Doha from 1 to 3 June 2009, A/CONF.213/RPM.2/1, Conclusions and Recommendations, No. 47 (page 10); "The Meeting recommended that the development of an international convention on cybercrime be considered", Report of the Asian and Pacific Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Bangkok from 1 to 3 July 2009, A/CONF.213/RPM.3/1, Conclusions and Recommendations, No. 29 (page 7); "The Meeting recommended the development of an international convention on cybercrime, as that would promote the priority of putting into place efficient national legislation, fostering international cooperation and building the skills of law enforcement personnel to address effectively the complex issues of cybercrime investigations, especially those of a cross-border nature", Report of the African Regional Preparatory Meeting for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, held in Nairobi from 8 to 10 September 2009, A/CONF.213/RPM.4/1, Conclusions and Recommendations, No. 40 (page 10).

[1452] Meeting Report, The Cybercrime Convention Committee, 2nd Multilateral Consultation of the Parties, 2007, page 2, available at: www.coe.int/t/e/legal_affairs/legal_co%2Doperation/combating_economic_crime/6_cybercrime/t%2Dcy/FINAL%20T-CY%20_2007_%2003%20-%20e%20-%20Report%20of%20the%20meeting1.pdf.

[1453] The term "phishing" originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" linked to popular hacker naming conventions, see *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. Regarding the phenomenon of phishing, see *Dhamija/Tygar/Hearst*, Why Phishing Works, available at: http://people.seas.harvard.edu/~rachna/papers/why_phishing_works.pdf; Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, available at: www.usdoj.gov/opa/report_on_phishing.pdf.

[1454] For an overview of the different legal approaches, see: *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the U.S.: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm. Regarding the economic impact, see for example the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[1455] There are two aspects that need to be taken into consideration in this context: To avoid redundancy, a new approach should focus on offences that are not intended to be covered within further amendments of the Convention on Cybercrime. The second aspect is related to the difficulties in finding a common position all countries can agree on. Based on the experiences with the negotiations of the Convention on cybercrime, it is likely that negotiations of criminalization that go beyond the standards of the Convention will run into difficulties.

[1456] Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1457] Regarding the need for international cooperation in the fight against cybercrime, see: *Putnam/Elliott*, International Responses to Cybercrime, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 35 *et seq*., available at: http://media.hoover.org/documents/0817999825_35.pdf; *Sofaer/Goodman*, Cybercrime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cybercrime and Terrorism, 2001, page 1 *et seq*., available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1458] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties which the dual criminality principle can cause within international investigations is currently addressed in a number of international conventions and treaties. One example is Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and surrender procedures between Member States (2002/584/JHA).

[1459] Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1460] See Convention on Cybercrime, Articles 23-35.

[1461] See *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141 *et seq.*

[1462] See above: § 2.6.7.

[1463] See Spam Issue in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1464] See Spam Issue in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1465] Regarding the network protocols, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1466] See, for example, the following surveys on national cybercrime legislation: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf; *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23 *et seq*., available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf; Legislative Approaches to Identity Theft: An Overview, CIPPIC Working Paper, No. 3, 2007; *Schjolberg*, The legal framework – unauthorized access to computer systems – penal legislation in 44 countries, available at: www.mosstingrett.no/info/legal.html.

[1467] Regarding the international dimension, see above: § 3.2.6.

[1468] With regard to the Convention on Cybercrime, see: Explanatory Report to the Convention on Cybercrime, No. 33.

[1469] Regarding concerns related to the speed of the ratification process, see *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 144.

[1470] See below: § 6.2.10.

[1471] See above: §§ 3.2.6 and 3.2.7.

[1472] The issue has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 stipulates: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 Ten-Point Action Plan highlights: "There must be no safe havens for those who abuse information technologies".

[1473] For details, see *Gercke*, National, Regional and International Legislative Approaches in the Fight Against Cybercrime, Computer Law Review International 2008, page 7 *et seq.*

[1474] For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm. For more information, see below: § 6.2.11.

[1475] Regarding filter obligations/approaches, see*: Zittrain/Edelman*, Documentation of Internet Filtering Worldwide, available at: http://cyber.law.harvard.edu/filtering/; *Reidenberg*, States and Internet Enforcement, University of Ottawa Law & Technology Journal, Vol. 1, No. 213, 2004, page 213 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=487965. Regarding the discussion on filtering in different countries, see*: Taylor*, Internet Service Providers (ISPs) and their responsibility for content under the new French legal regime, Computer Law & Security Report, Vol. 20, Issue 4, 2004, page 268 *et seq.*; Belgium ISP Ordered By The Court To Filter Illicit Content, EDRI News, No. 5.14, 18.06.2007, available at: www.edri.org/edrigram/number5.14/belgium-isp; *Enser*, Illegal Downloads: Belgian court orders ISP to filter, OLSWANG E-Commerce Update, 11.07, page 7, available at: www.olswang.com/updates/ecom_nov07/ecom_nov07.pdf; *Standford*, France to Require Internet Service Providers to Filter Infringing Music, 27.11.2007, Intellectual Property Watch, available at: www.ip-watch.org/weblog/index.php?p=842; *Zwenne*, Dutch Telecoms wants to force Internet safety requirements, Wold Data Protection Report, issue 09/07, page 17, available at: http://weblog.leidenuniv.nl/users/zwennegj/Dutch%20telecom%20operator%20to%20enforce%20Internet%20safety%20requirements.pdf; The 2007 paper of IFPI regarding the technical options for addressing online copyright infringement, available at: www.eff.org/files/filenode/effeurope/ifpi_filtering_memo.pdf. Regarding self-regulatory approaches,

see: ISPA Code Review, Self-Regulation of Internet Service Providers, 2002, available at: http://pcmlp.socleg.ox.ac.uk/selfregulation/iapcoda/0211xx-ispa-study.pdf; *Zittrain*, Harvard Journal of Law & Technology, 2006, Vol. 19, No. 2, page 253 *et seq.*

1476 See: *Poullet*, The Yahoo! Inc. case or the revenge of the law on the technology?, available at: *www.juriscom.net/en/uni/doc/yahoo/poullet.htm*; *Goldsmith/Wu*, Who Controls the Internet?: Illusions of a Borderless World, 2006, page 2 *et seq.*

1477 The OpenNet Initiative is a transatlantic group of academic institutions that reports about Internet filtering and surveillance. Among others, the Harvard Law School and the University of Oxford participate in the network. For more information, see: www.opennet.net.

1478 *Haraszti*, Preface, in Governing the Internet Freedom and Regulation in the OSCE Region, available at: www.osce.org/publications/rfm/2007/07/25667_918_en.pdf.

6. 法律对策

本章通过解释对某些行为进行定罪的法律方法，概况介绍了对网络犯罪现象的法律对策。[1479] 只要有可能，就尽量采用国际性解决方法。如果无法采用国际性解决方法，将提供国家或地区性解决方法的例子。

6.1 定义

Bibliography (selected): *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.; *Macagno*, Definitions in Law, Bulletin Suisse de Linguistique Appliquée, Vol. 2, 2010, page 199 et seq, available at: http://ssrn.com/abstract=1742946.

6.1.1 定义的功能

定义是各种国家和区域法律框架中一种常见的要素。但是，区别这些定义的不同功能是重要的。在法律中，通常可分为两种定义：说明定义和法定定义。[1480] 说明定义用于解释有多重含义的字词的含义，而法定定义则旨在将有待法律规定的定义转化为某个字词的具体定义。[1481] 以下概述并未区分这两种类型的定义。

区域性法律框架和示范法并不仅仅遵循与定义有关的不同概念，在涉及定量问题时亦是如此。例如，《网络犯罪公约》只有 5 个定义 [1482]，而《HIPCAR 网络犯罪示范立法文本》中有 20 个定义。

6.1.2 接入提供商

接入提供商发挥着重要作用，因其使得用户可以接入互联网。在网络犯罪法律中，“接入提供商”一词既用于责任监管 [1483]，也可以用于案件调查中——特别是合法的通信监听。[1484] HIPCAR 网络犯罪示范立法文本中给出了有关访问服务提供商的定义。

定义

3. *(1)* 接入提供商指在通信网络中通过传送业务用户提供的信息或向业务用户传送信息的方式，提供电子数据传输业务或提供通信网络接入的任意自然人或法人。

[…]

这是一个广义的条款，因为它涉及到企业提供商和只为其员工或专用网络运营商提供接入服务的公司。当这些方法可用并广泛应用与责任控制时，如果这种定义还应用于诉讼法，则会产生一些问题（这并非 HIPCAR 网络犯罪示范立法文本制定者的初衷）。

6.1.3 缓冲提供商

缓冲提供商能提供一项重要的服务，以增加访问公共内容的速度。对于需要参与责任控制[1485]的高速缓存提供商，《HIPCAR 网络犯罪示范立法文本》起草者决定引入如下定义。

定义
3. *[…]*
(2) 高速缓存提供商指的是以自动地、过渡地和临时地存储信息的方式提供电子数据传输服务的任何自然人和法人，目的是使信息在提出请求的服务用户之间的传输更有效；
[…]

如同接入提供商的定义一样，起草者并未将该款的应用限于商业操作。因此，该规定也涵盖公司和专用网络运营商。

6.1.4 儿童

“儿童”一词与儿童色情的定罪密切相关。[1486] 该词也用于为向未成年人提供特定内容（如成人色情物品）定罪规定的背景下。[1487] 其中最为常用的一个定义述于 1989 年的《联合国儿童权利公约》中。

在本《公约》中，儿童指 18 岁以下的人，除非根据适用于儿童的法律，法定成年年龄更低。

数项针对网络犯罪的法律框架和示范法（如 2011 年有关打击儿童色情的欧盟指令 [1488]、2007 年《欧洲理事会保护儿童公约》[1489] 以及 2009 年《HIPCAR 网络犯罪立法示范文本》[1490] 均包含了类似的定义。《欧洲理事会保护儿童公约》并未定义儿童，仅对儿童色情进行了定义。

6.1.5 儿童色情

儿童色情是几种涉及非法内容的违法行为之一，世界上大多数国家都认为这是一种犯罪行为。[1491] 由于区分合法的与性相关的作品和儿童色情资料有困难，所以，某些法律框架给出了儿童色情资料的定义。

就这点而言，法律制定者面临的困境之一是避免在不同年龄类别之间产生冲突，目的在于避免当结婚年龄或性内容以及年龄限制在儿童色情的定义中存在分歧时，可能存在的非故意犯罪。[1492] 例如，如果儿童色情资料被定义为 18 岁以下的人的性行为的视觉描绘，同时，如果允许接触性内容和结婚的年龄是 16 岁，两个 17 岁的儿童可以结婚或存在性关系，但他们制作描绘性行为的图像和视频会被认定为严重的犯罪（儿童色情的产物）。[1493]

《买卖儿童、儿童卖淫和儿童色情中的儿童权益公约任择议定书》第 2 条 c) 款给出了儿童色情资料的定义。

第 2 条
出于本议定书的目的：
[…]
(c) 儿童色情资料系指无论以何种形式，对儿童参与真实的或模仿的直接性行为的任何描绘，或出于性目的对儿童的性部分进行的任何描绘。

任择议定书》中给出的定义没有明确涵盖虚构的儿童色情资料的形式，如写真图像。为了确保这类内容也纳入其中，某些法律框架，如欧洲理事会《网络犯罪公约》，已经对儿童色情资料的定义进行了补充。

第 9 条–涉及儿童色情资料的违法行为

[…]

(2) 出于上述第 1 款的目的，“儿童色情资料”一词应包括色情作品的视觉描绘：

a) 未成年人参与直接的性行为；

b) 看上去像未成年人的人参与直接的性行为；

c) 反映未成年人直接参与性行为的写真图像；

(3) 出于上述第 2 款的目的，“未成年人”一词应包括所有 18 岁以下的人。但某些国家可能有较低的年龄限制，但不应低于 16 岁。

[…]

第 9 条第 2 款对视觉上描绘儿童色情活动的作品给出了三个分款：未成年人参与直接性行为、看上去像未成年人的人参与直接的性行为以及反映未成年人直接参与性行为的写真图像。

就这点而言，《网络犯罪公约》扩展了《欧盟公约任择议定书》中给出的定义，另一方面，在两个重要方面限制了其实用性。

尽管《网络犯罪公约》的起草者强调关于年龄[1494]的统一国际标准，但《网络犯罪公约》允许签约国有不同的年龄限制，但不得低于 16 岁。

《任择议定书》中所给出的定义的第二个主要不同点在于欧洲理事会《网络犯罪公约》着重强调视觉描绘。儿童色情资料不一定全是图像或视频，也可以是音频文件。[1495]而在第 9 条中指的是针对儿童的“直觉描绘作品”，该定义没有包括音频文件。

因此，多数当今的立法，如《HIPCAR[1496]网络犯罪的立法文本》[1497]仍沿用《欧盟网络犯罪任择议定书》中的概念，而不是欧洲理事会《网络犯罪公约》，避免使用“视觉”一词。

定义

3.

[…] (4)儿童色情资料系指描绘、展示或描述下列情形的色情作品：

a) 儿童参与直接的性行为；

b) 看起来像儿童的人参与直接的性行为

c) 描绘儿童参与直接性行为的图像；

包括但不限于任何音频、视频或文本型色情作品。

签约国可以不通过执行(b)款和(c)款来限制定罪。

《欧盟反对儿童色情资料指令》（2011）[1498]和《欧洲保护儿童公约》中也给出了儿童色情资料的定义。[1499]

6.1.6 计算机数据

计算机技术的不断应用以及数据数字化的趋势使得计算机数据的关联性越来越强。因此，计算机数据已成为攻击的主要目标，攻击的范围从数据干扰[1500]到数据刺探。[1501]各种地区性框架都对计算机数据进行了定义。其中一个具体的例子就是《英联邦计算机与计算机相关犯罪示范法》中给出的定义。

定义
3．在此法案中，除非出现相反的动机，不然：
“计算机数据”系指以适于在计算机系统内进行处理的形式对任何事实、信息或概念的表述，包括能够使计算机系统运行的一段程序；
[…]

欧洲理事会《网络犯罪公约》（2001）[1502]、《关于针对信息系统攻击的框架决议》（2005）[1503]、《ECOWAS 对抗网络犯罪指令》（2008）[1504] 和《HIPCAR 关于网络犯罪的示范立法文本》[1505]中也给出了类似的定义。

6.1.7 计算机数据存储设备

存储设备在网络犯罪（潜在的数据干扰和证据捕获）中发挥着重要的作用。包含此类定义的地区性框架的具体实例是《英联邦计算机与计算机相关犯罪示范法》第 3 节。

定义
3．
[…]
“计算机数据存储介质”系指能够不借助于任何其他物体或设备对信息进行复制的物体或物质（例如磁盘）
[…]

《HIPCAR 示范立法文本》[1506]也给出了类似的定义。

6.1.8 计算机系统

在网络犯罪法中，“计算机系统”一词应用于刑法和诉讼法中。计算机系统可以是攻击的目标；犯罪时，计算机系统可以作为一种工具，最终又作为被抓获的证据。因此，大多数现行地区性框架和示范法都有这样的定义。具体的实例是《英联邦计算机与计算机相关犯罪示范法》（2002）第 3 节给出的定义：

定义
3．
[…]
“计算机系统”系指一个设备或一组内部连接或关联的设备，包括互联网，多数计算机系统都按照程序来执行数据自动处理或实现任何其他功能；
[…]

不寻常的是，定义中提到了“互联网”。互联网被广泛解释为互相连接的网络系统。[1507] 因此，从技术层面上看，互联网本身不是一个计算机系统，而是一个网络，因而不应包括在计算机系统的定义中，但可以包括在计算机网络的定义中。然而，个别法律框架的制定者仍沿用《英联邦示范法》中的定义，将互联网纳入到计算机系统的定义中。

欧洲理事会《网络犯罪公约》（2001）[1508]、《关于针对信息系统攻击的框架决议》（2005）[1509]、《ECOWAS 对抗网络犯罪指令》（2008）[1510] 和《HIPCAR 关于网络犯罪的示范立法文本》[1511]中也给出了类似的定义。

6.1.9 重要基础设施

由于在运行重要基础设施过程中不断适应计算机和网络技术，这类基础设施有可能成为攻击的目标。[1512] 考虑到这类攻击的潜在威胁，一些现行法律框架包含对攻击重要基础设施行为进行了特殊量刑或加重处罚，同时也给出了具体的定义。具体例子见《HIPCAR 示范立法文本》中给出的定义。

> **定义**
> 3.
> [...]
> (8) 重要基础设施系指对国家至关重要的计算机系统、设备、网络、计算机程序、计算机数据，使这类系统和资产丧失能力或遭到破坏有可能弱化安全性，包括国家或经济的安全、国家公共卫生设施安全或几方面共同的安全性；
> [...]

6.1.10 密码学

罪犯使用加密技术可以严重阻碍获取相关证据。[1513] 因此个别国家实施了解决加密技术应用问题的立法和有关执法调查的文书。[1514] 但是，从不同解决网络犯罪的地区性法律框架来看，只有《非洲联盟网络安全公约》（草案）[1515] 在第 I-1 条中给出了密码学的定义。

> 8) 密码学系指出于保证机密性、鉴别、完整性和不可抵赖性的目的对信息进行保护的科学；

6.1.11 设备

“设备”一词专门用于针对“非法设备”的定罪过程。[1516] 鉴于这类设备可能广泛传播并应于实施犯罪的潜在风险，个别地区性法律框架的制定者决定设置对使用非法设备的某些行为定罪的条款。不同于欧洲理事会《网络犯罪公约》和《英联邦示范法》（都使用“设备”一词），《HIPCAR 示范立法》在第 3 条对该词做出了定义。

> **定义**
> 3.
> [...]
> (9) 设备包括但不限于：
> a) 计算机组件，如，图形卡、内存、芯片等；
> b) 存储部件，如，硬盘驱动器、存储卡、光盘、磁带等；
> c) 输入设备，如，键盘、鼠标、轨迹板、扫描仪、数码相机等；
> d) 输出设备，如，打印机、监视器等；
> [...]

这是一个典型的描述性定义，因为该条款明确指出了设备的定义应不限于所列出的部件（“包括但不限于”）。根据对非法设备定罪的基本条款[1517]，“设备”一词还应包括计算机程序。

6.1.12 妨碍

在广泛使用电子商务的信息社会和信息经济中使用计算机是非常必要的。妨碍计算机系统正常运行的攻击活动会严重干扰社会和经济。因此，很多地区性法律框架认定妨碍计算机系统正常运行是有罪的。[1518]《关于网络犯罪的 HIPCAR 示范立法文本》在第 3 条对“妨碍”一词做出了定义。

> **定义**
> 3.
> […]
> (10) 妨碍计算机系统的活动包括但不限于：
> a) 切断计算机系统的供电电源；
> b) 对计算机系统进行电磁干扰；
> c) 通过各种手段破坏计算机系统；
> d) 输入、传输、损坏、删除、恶化、更改或压缩计算机数据；
> […]

该定义强调妨碍活动包括物理干扰（如，切断电源）以及对数据的非法操作（输入计算机数据）。

6.1.13 主机提供商

主机提供商在防止网络犯罪中的具有很重要的作用，因为他们的服务会被用于存储非法内容。因此，不同的地区性法律框架都会考虑网络服务提供商责任的问题。[1519]然而，主要的地区性法律框架并没有给出主机提供商的定义。但在《关于网络犯罪的 HIPCAR 示范立法文本》中给出了主机提供商的定义。

> **定义**
> 3.
> […]
> (11) 主机提供商系指通过存储服务用户提供的数据来提供电子数据传输服务的任何自然人和法人；
> […]

该定义也包括针对商业服务提供商和私人操作员的规定。因此，即使是能使其他人在网站上存储信息私人网站的操作员也涵盖在相应的责任范围内。

6.1.14 超链接

由于通常只有主机提供商、访问服务提供商和高速缓存提供商列入网络服务提供商（ISP）的子类中，所以个别法律框架对其他服务，如搜索引擎[1520]和超链接，做出了专门的规定。在这方面，《关于网络犯罪的 HIPCAR 示范立法文本》对超链接做出了定义。

定义
3.
[...]
(12) 超链接系指某个元素，如符号、单词、短语、句子或图像的特征和属性，这些元素包含并且指向其他来源的信息，当执行时可以显示这些信；
[...]

这个定义是广义的，包含各种类型的超链接，如深度链接。

6.1.15 监听

监听一词常用于对非法监听[1521]定罪的实体刑法和关于合法通信监听的刑事诉讼法中。一些地区性法律框架，如欧洲理事会《网络犯罪公约》和《英联邦示范法》包含有关非法监听和合法监听的条款，而这些法律框架并没有对监听做出定义。但《关于网络犯罪的 HIPCAR 示范立法文本》对这一名词做出了定义。

定义
3.
[...]
(13) 监听包括但不限于通过有线、无线、电子、光、磁、口述或其他方式，在通过任何技术设备传输的过程中获取、浏览和捕获任何计算机通信数据；
[...]

6.1.16 干扰

干扰是一个标准名词，常用于很多有关网络犯罪的法律条款中。具体的实例有数据干扰[1522]和系统干扰[1523]。但是，在一些地区性法律条款中，该词只用于某些条款的标题，但没有对犯罪行为的细节进行描述。因此，大多数法律框架和示范法都没有进一步定义这个词。

6.1.17 群发电子邮件

所有电子邮件中，有相当数量的是垃圾邮件。因此，在一些国家以及当前的示范法中都有关于对发送垃圾邮件行为定罪的法律条款。[1524]在这些条款中用到的关键词是“群发电子邮件”。《关于网络犯罪的 HIPCAR 示范立法文本》对这一名词做出了定义。

定义
3.
[...]
(14) 群发电子邮件系指一份包含电子邮件，并且同时发送给成千上万的收件人邮件信息；
[...]

6.1.18 远程取证软件

很多现行的和先进的法律框架包含在某些情况下授权执法机构应用先进的取证工具的诉讼条款，例如键盘记录程序。[1525]《关于网络犯罪的 HIPCAR 示范立法文本》对远程取证软件做出了定义。

> **定义**
> 3.
> […]
> (15) 远程取证软件系指一种安装在计算机系统上、用于执行（包括但不限于）键盘记录或 IP 地址传输任务的调查软件；
> […]

在讨论使用专为加勒比海地区制定的 HIPCAR 标准过程中，在太平洋地区有人指出，为了覆盖整个远程解决方案的应用范围，相对于软件而言，“工具”这个词（也包括硬件解决方案）更合适。

6.1.19 扣押

不论对于传统犯罪还是网络犯罪，扣押都是用于收集证据最为重要的调查手段之一。[1526]《英联邦计算机与计算机相关犯罪示范法》第 11 节对扣押做出了定义。

> 此部分的定义
> […]
> 11.在此部分中：
> […]
> “扣押”包括：
> (a) 制作、保留计算机数据的备份，包括使用现场设备；
> (b) 在可访问的计算机中使计算机数据不可访问或移除计算机数据
> (c) 打印计算机数据的输出结果。
> […]

这一包含三个子款的定义在制定《HIPCAR 关于网络犯罪的示范立法文本》过程中做了进一步的补充。第 3 节（16）条给出了完整的定义。

> **定义**
> 3.
> […]
> (16) 扣押包括：
> *a.* 启动所有现场计算机系统和计算机数据存储介质；
> *b.* 制作、保留计算机数据的备份，包括使用现场设备；
> *c.* 保证存储的计算机数据的完整性；
> *d.* 可访问的计算机中使计算机数据不可访问或移除计算机数据；
> *e.* 打印计算机数据的输出结果；或
> *f.* 查封或保护计算机系统或计算机数据存储介质；
> […]

欧洲理事会《网络犯罪公约》采用不同的定义方法，在其条款中包含了扣押的不同要素。[1527]

6.1.20 服务提供商

服务提供商是用于描述不同类型的提供互联网服务的提供商的定义。如上所述，不同地区性法律框架包含针对服务提供商的法律条款（例如，关于不同类型服务提供商责任的条款或服务提供商要求执法支持诉讼条款）。并不是所有这些都对不同类型的服务提供商有区别。因此，那些地区性法律框架，包括服务提供商的定义，都没有专门的区分。欧洲理事会《网络犯罪公约》给出了一个具体的定义。

第 1 条–定义

[…]

c) “服务提供商”系指：

i. 任何通过计算机系统为其服务用户提供通信能力的公共或私人团体；

ii. 任何处理或存储参与通信服务的计算机数据的其他团体或这类服务的用户；

《英联邦计算机与计算机相关犯罪示范法》（2002）[1528]和《关于网络犯罪的 HIPCAR 示范立法文本》（2009）[1529]都有类似的定义。

6.1.21 流量数据

流量数据是一种数据类型，用于为某些地区性法律框架和示范法提供专门的调查工具。[1530]。因此，这些地区性法律框架和示范法中都对流量数据做出了定义。《英联邦计算机与计算机相关犯罪示范法》第 3 节给出了该定义的一个具体实例。

定义

3.

[…]

“流量数据”系指具有下列特征的计算机数据：

(a) 与利用计算机系统的通信有关；

(b) 由通信链路中的计算机系统产生；

(c) 可以看出通信的源地址、目的地址、路径、时间日期、大小、上述服务的持续时间或类型。

欧洲理事会《网络犯罪公约》（2001）[1531]和《关于网络犯罪的 HIPCAR 示范立法文本》（2009）[1532]也给出了类似的定义。

6.2 实体刑法

参考书目（节选）： ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, Entertainment Law Review, 2002; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991; *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Broadhurst*, Development in the global law enforcement of cybercrime, in Policing: An International Journal of Police Strategies and Management, 29(2), 2006; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002; *Decker*, Cyber Crime 2.0: An

Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81; *El Sonbaty*, Cyber Crime – New Matter or Different Category?, published in: Regional Conference Booklet on Cybercrime, Morocco 2007; *Gercke/Tropina*, from Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Gercke*, Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, Computer Law Review International, 2010; *Gercke*, National, Regional and International Approaches in the Fight against Cybercrime, Computer Law Review International, 2008, Issue 1; *Gercke*, Cybercrime Training for Judges, 2009; *Gercke*, How Terrorist Use the Internet in Pieth/Thelesklaf/Ivory, Countering Terrorist Financing, 2009; *Goyle*, Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, CRS Report, 2008, 97-1025; *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527; *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf; Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.*, available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf; *Lavalle*, A Politicized and Poorly Conceived Notion Crying Out for Clarification: The Alleged Need for Universally Agreed Definition of Terrorism, Zeitschrift fuer auslaendisches oeffentliches Recht und Voelkerrecht, 2006, page 89 *et seq.*; *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999; *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11; *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact and Prevention, Youth & Society, Vol. 34, 2003; *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf; *Parsonage*, Web Browser Session Restore Forensics, A valuable record of a user's internet activity for computer forensic examinations, 2010, available at: http://computerforensics.parsonage.co.uk/downloads/WebBrowserSessionRestoreForensics.pdf; Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analysed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005; *Schjolberg/Ghernaouti-Heli*, A Global Protocol on Cybersecurity and Cybercrime, 2009; *Tedford/HerbeckHaiman*, Freedom of Speech in the United States, 2005; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement Act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII; *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, 2001; *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm; *Stol/Kaspersen/Kerstens/Leukfeldt/Lodder*, Filteren van kinderporno op internet, 2008; *Vogel*, Towards a

Global Convention against Cybercrime, First World Conference of Penal Law, ReAIDP/e-RIAPL, 2008, C-07; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33; *Walden*, Computer Crimes and Digital Investigations, 2006; *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2; *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729; *Wolak/ Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf.

6.2.1 非法访问（黑客行为）

随着计算机网络的发展，能够连接到其他计算机并且能够为用户提供对其他计算机系统的访问，计算机已被黑客们用于犯罪。[1533] 黑客的动机已出现实质性变化。[1534] 黑客不必出现在犯罪现场；[1535] 他们只需绕过网络的安全保护措施即可。[1536] 在许多非法访问的案例中，即使是在同一幢建筑物内，保护网络硬件物理设施的安全系统也比保护网络上敏感信息的安全系统更为复杂。[1537]

非法访问计算机系统使计算机操作者无法以一种不受干扰和不受约束的方式来管理、操作和控制其系统。[1538] 保护的目的是维护计算机系统的完整性。[1539] 至关重要的是区分非法访问和后续的违法行为（如数据刺探 [1540]），原因是法律条款对保护的着重点有区别。在大多数情况下，非法访问（在这些情况下，法律着重于保护计算机系统本身的完整性）并非最终目标，而只是进一步犯罪的第一步，比如修改或获取储存的数据（在这些情况下，法律着重于保护数据的完整性和机密性）。[1541]

问题是，除了对后续的违法行为应当予以定罪之外，对其第一步，即非法访问行为是否应当也予以定罪？[1542] 从国家层面的各种对非法访问计算机定罪的方法分析表明，一些已制定的规定有时候将非法访问与后续的违法行为混为一谈，或者仅对造成严重侵犯的非法访问给予定罪。[1543] 有些国家对单纯的非法访问也进行定罪，而另一些国家则只对以下行为予以定罪，即被访问系统受到安全措施的保护、或者作案者具有恶意、或者数据已被作案者获取、修改或破坏。[1544] 还有一些国家不对非法访问本身定罪，而只对后续的违法行为定罪。[1545] 反对对非法访问本身定罪涉及以下情形，即单纯的侵入并未造成任何危险，或者“黑客”行为反而使目标计算机系统察觉到了安全漏洞和弱点。[1546]

欧洲理事会《网络犯罪公约》

欧洲理事会《网络犯罪公约》有一条关于非法访问的规定，该规定通过对未授权的系统访问进行定罪，来保护计算机系统的完整性。考虑到与国家层面上方法不一致，[1547] 《网络犯罪公约》提供了限制的可能性 — 至少在大多数情况下是这样 — 使得一些没有针对非法访问进行立法的国家能够对这一问题保留更为宽松的法律。[1548] 该规定的目的在于保护计算机系统的完整性。

条款

第 2 条—非法访问

当针对整个计算机系统或其任何部分的访问属于未经授权故意访问时，各方应采用依据本国法律认定犯罪行为所需的法律手段和其他手段。签约方可以认定的违法行为是通过侵害安全措施，或侵害连接到另一计算机系统的计算机系统，并带有获得计算机数据的意图或其他不诚实的意图的行为。

涉及的行为

“访问”这一术语并没有规定一种特定的通信手段，而是可扩展的，并且对下一步的技术开发开放。[1549] 它应包括可用于进入另一个计算机系统的所有手段，包括互联网攻击，[1550] 以及非法访问无线网络。甚至法律条款还涵盖对没有连接到任何网络的计算机的访问（例如，通过绕过密码保护措施）。[1551] 这种广义的方法意味着非法访问不仅包括未来的技术发展，而且也包括内部人员和员工对秘密数据的访问。[1552] 第 2 条第二句说明了限制对经由网络的非法访问进行定罪的可能性。[1553]

因此，以一种对未来开发保持开放的方式定义了非法行为和受保护的系统。《解释性报告》将硬件、组件、储存的数据、目录、通信流量以及与内容有关的数据列为可被访问的计算机系统组件的例子。[1554]

主观因素

与欧洲理事会《网络犯罪公约》定义的所有其他违法行为一样，第 2 条要求违法者是故意实施了违法行为。[1555] 《网络犯罪公约》并没有包含对“故意”这一术语的定义。起草者在《解释性报告》中指出，“有意”应当在国家层面上进行定义。[1556]

未获授权

根据《公约》第 2 条的规定，只有当访问是“未授权”时，对计算机的访问才可被起诉。[1557] 对允许公众自由和公开访问的系统进行访问，或者获得了系统所有者或其他权限所有持有者授权的访问，则不属于“未授权”。[1558] 除了自由访问这一问题，还应解决安全测试程序的合法性问题。[1559] 网络管理员以及为确定安全措施上可能的缺陷而对计算机系统保护措施进行测试的安全公司，都对因非法访问而定罪的可能性保持警惕。[1560] 尽管这些专业人士通常获得所有者的许可而操作，并且是合法开展工作的，但《网络犯罪公约》的起草者强调，“获得所有者或操作员授权而对计算机系统安全性进行测试或保护，[...]视为获得授权”。[1561]

当犯罪的受害者向违法者交出密码或类似的访问代码时，并不一定意味着违法者访问受害者的计算机系统时是经授权的访问。如果通过一种成功的社会工程方法，[1562] 违法者说服受害者透露密码或访问代码，那么有必要验证受害者提供的授权是否涵盖违法者所实施的行为。[1563] 情况一般并非如此，因此违法者的行为是未授权的。

限制与保留

作为一种可替代的广义方法，《网络犯罪公约》能够用附加要素来限制定罪，其内容列于定义的第二句。[1564] 《网络犯罪公约》的第 42 条规定了如何使用这一保留概念。[1565] 可能存在的保留涉及安全措施、[1566] 获取计算机数据的特殊意图、[1567] 其他为犯罪过失辩护的不诚实意图或要求通过网络对计算机系统实施违法行为。[1568] 《欧盟 [1569] 关于针对信息系统攻击的框架决议》[1570] 中可以找到一种类似的方法。

《英联邦计算机与计算机相关犯罪示范法》

在 2002 年版的《英联邦示范法》的第 5 节中可以找到一种类似的方法。[1571] 类似于欧洲理事会《网络犯罪公约》，这一规定保护的是计算机系统的完整性。

非法访问 5.

如果某人故意或没有合法或正当理由访问整个或部分计算机系统并实施应受处罚的违法行为，在定罪时，可处以不超过[一定期限]的监禁，或者不超过[一定数量]的罚款，或者两项并罚。

第 5 节所采用的方法类似于欧洲理事会《网络犯罪公约》第 5 条的方法。与《英联邦示范法》的主要区别在于：《英联邦示范法》第 5 节未包含可保留的选择方案。

《欧盟关于针对信息系统攻击的指令》

2013 年出版的《欧盟关于针对信息系统攻击的指令》[1572]在第 3 条规定了针对非法访问信息系统进行定罪的方法。

第 3 条 — 非法访问信息系统

1. 成员国须采取必要的措施，以确保故意以侵害安全性措施的方式非授权访问整个或部分信息系统是可处罚的犯罪行为，至少对成年人作案的案件是这样。

2. 各成员国只有在违法行为被指控为破坏安全设施时方可确定第 1 段中指出的行为是有罪的。

上述条款是依照欧洲理事会《网络犯罪公约》确定的标准制定的。[1573] 与《网络犯罪公约》的首要主要区别之一在于成员国可以对成年人案件的定罪进行限制。在这种情况下，框架决议明确指出未成年人案件应不属于此类。[1574] 区别之二在于第 3 条限制了在对现有安全性措施构成侵害的情况下的可适用性。在《网络犯罪公约》中，这仅为一项非强制性限制措施。

《斯坦福国际公约草案》

1999 年出版的非正式的 [1575]《斯坦福公约草案》将非法访问视为签约国应予以定罪的违法行为之一。

条款

第 3 条— 违法行为

1. 根据这一《公约》，如果任何人在未获得合法授权、许可或同意的前提下非法、故意从事以下任何行为，那么认为就是在实施违法行为：

[...]

(c) 以明显、明确的方式进入一个访问受限的网络系统；

[...]

涉及的违法行为：

条款草案与欧洲理事会《网络犯罪公约》第 2 条有许多相似之处。两者都要求是未获授权/未授权而实施的有意行为。这种情况下，草案条款的要求（“未获得合法的授权、许可或同意”）比《网络犯罪公约》中使用的“未授权”[1576] 这一术语更加精确，而且明确着眼于融入自我防卫的概念。[1577] 与《公约》的主要差别在于，草案条款使用了“网络系统”这一术语。网络系统在《公约》草案的第 1 条第 3 段中定义。它包括用于转发、传输、协调或控制数据或程序通信的任何计算机或计算机网络。该定义与《网络犯罪公约》第 1 条 a) 中提供的“计算机系统”这一术语有许多相似之处。[1578] 尽管《公约》草案指的是与数据交换有关的行为，并因此主要着重于基于网络的计算机系统，但两个定义都包括了互联的计算机以及单机。[1579]

6.2.2 非法保留

计算机系统的完整性不仅因非法进入而被破坏，还会因权限失效后继续使用而别破坏。由于这种情况下计算机系统被非法访问，所以，很难用上述条款对非法访问计算机系统定罪。

欧洲理事会

欧洲理事会《网络犯罪公约》认定非法进入计算机系统术语犯罪行为，但不包括非法保留计算机系统的使用权限。然而，在《公约》协商过程中讨论过非法保留。1998 年，《网络犯罪公约》第四版草案编写完成时，仍包含这一要素。

> **第 2 条—** 针对计算机数据和系统机密性、完整性和可用性的违法行为
>
> 当认定故意实施下列行为时，各签约国应在本国法律的基础上，采用此类立法措施及其他措施作为认定其为违法行为的必要依据：
>
> [...]
>
> 1*bis* 当某人意识到情况的[不合法性]时，利用人为故障退出已经非故意无权访问了的部分或全部计算机系统。
>
> [...]

但 2001 年待签的《网络犯罪公约》的最终版不再包含这一规定。

实例

最近，有些立法，如，《HIPCAR[1580] 网络犯罪立法文本》[1581] 包含解决这类问题专门的条款。第 5 节规定非法保留计算机系统属于犯罪。类似于对非法访问定罪，受保护的合法利益是计算机系统的完整性。

> **非法保留**
>
> 5. (1) 没有合法借口或理由或超出合法借口或理由的范围，故意登陆某一计算机系统或一部分计算机系统，或继续使用某一计算机系统的人犯有应受处罚的罪行，定罪时，可以处以不超过[具体期限]的监禁，或处以不超过[具体数额]的罚款，或二者并罚。
>
> (2) 各国可以决定对单一的未授权保留不予处罚，前提是要有其他行之有效的补救措施。另外，各国可以要求对破坏安全措施或故意获取计算机数据或其他不诚实企图进行定罪。

该条款反映的是计算机系统完整性遭到破坏的原因不仅是未获授权进入计算机系统，还应是在授权过期情况下继续使用计算机系统。保留要求违法者仍继续进入计算机系统。可以是这样的情形，例如，违法者保留登陆状态或继续操作进行操作。违法者理论上有可能登陆到计算机系统这一事实是不够的。第 54 节要求违法者正在故意实施违法行为。不包括轻率行为。另外，第 54 节的规定只对违法者在“没有合法借口或理由”情况下实施的行为才属于犯罪行为。

6.2.3 非法获取计算机数据

欧洲理事会《网络犯罪公约》、《英联邦示范法》和《斯坦福国际公约》（草案）只是针对非法监听提出了解决方案。[1582] 欧洲理事会《网络犯罪公约》第 3 条是否适用于除在数据传输过程中利用监听实施的违法行为之外的其他案件还是个问题。正如以下所述，[1583] 人们带着浓厚的兴趣，对非法访问存储在硬盘中的信息是否属于《网络犯罪公约》的范畴这一问题进行了讨论。[1584] 因为需要传输过程，所以，《网络犯罪公约》第 3 条除了考虑传输过程中的监听外，有可能没有考虑到数据刺探的形式。[1585] 正如《网络犯罪公约》（第 9 版草案）提到了违法数据刺探的相关性一样，这是相当有趣的事。

在这种情况下，一个经常讨论的问题是：对于非法访问的定罪是否会弱化对进行不必要的数据刺探行为的定罪。如果罪犯通过合法途径访问计算机系统（例如，有人要求他去维修计算机），而在这种（违反有限法律的）情况下违法者从系统中复制了文件，这种行为不属于为非法访问定罪的法律条款的范畴。[1586]

假设这类重要数据存储在计算机系统中，那就有必要评估现有机制是否足以保护数据，或是否有其他刑法条款足以保护用户不受到数据刺探的攻击。[1587] 如今，计算机用户可以使用各种硬件设备和软件工具来保护秘密信息。他们可以安装防火墙和访问控制系统或对存储的信息进行加密，以减小数据刺探活动的风险。[1588] 尽管可以使用用户友好型设备并且不需要用户有太多的知识，但是，真正有效地保护计算机系统中的数据通常要求很多知识，而很少用户有这样的知识。[1589] 存储特别是存储在私人计算机系统中的数据，通常没有足够的防护措施来防止数据刺探活动。因此，刑法条款可以提供附加的保护。

有些国家已决定通过对数据刺探活动定罪的形式和技术手段扩大有效保护的范围。主要有两种方法。有些国家采用限制较小的方法，只对获取特定秘密信息的数据刺探定罪 — 美国法典标题 18（第 1831 段）给出了一个具体的实例，该实例定罪为经济间谍。该条款不仅涉及数据刺探活动，也考虑到利用其他手段获取秘密信息。

美国法典

§ 1831 – 经济间谍

(a) 一般情况 — 任何人估计或明知其违法行为会对外国政府、外国机构或外国代理人有利而故意实施下列行为：

(1) 盗窃，或在没有合理授权的情况下取得、带走或隐藏商业秘密，或通过诡计、欺诈或骗术获取商业秘密；

(2) 在没有授权的情况下拷贝、复制、速记、绘制、拍照、下载、上传、更改、破坏、影印、翻印、传输、递送、发送、邮寄、电传或转送商业秘密；

(3) 在确知其行为等同于盗窃或无授权占有、获取或修改的情况下接收、购买或处理商业秘密；

(4) 企图实施(1)-(3)所述的任何一种犯罪行为；或

(5) 与一名或多名其他人共谋实施(1)-(3)所述的任何一种犯罪行为，而共谋者所做的一切都影响到共谋的结果，除(b)款的规定外，这种行为应当处以 50 万美元的罚款或 15 年以下的监禁或并罚。

(b) 组织 — 任何实施(a)款所述的犯罪行为的组织应处以 1 千万美元的罚款。

§ 1831 已引入到 1996 年颁布的《经济间谍法》。[1590] 1996 年以前，经济间谍只是在很大程度上不一致的州法律下才认定为犯罪行为。[1591]《经济间谍法》认定标题 18 中所列的两种商业秘密侵占行为为犯罪行为 — 为外国政府、机构和代理牟利的商业秘密盗窃；为经济利益实施的商业性商业秘密盗窃，不论其是否为外国政府、机构和代理牟利。[1592] 尽管该条款将重点放在内容（商业秘密）内容的保护上，并没有要求具体的形式（计算机数据），所以，这不仅是传统犯罪，还是计算机犯罪。[1593] 总之，美国法典标题 18 中的 § 1030(a)(2)款也适用于这类情况。[1594]§ 1831(a)(2)-(5)。所涉及的行为属于计算机犯罪。

《HIPCAR 网络犯罪立法文本》

《HIPCAR [1595] 网络犯罪立法文本》第 8 节 [1596] 给出了数据刺探的另一实例。

数据刺探

8. (1) 在没有合法借口或理由、或超出合法借口或理由范围的情况下故意为自己或他人获取不属于他自己而且为防止未授权访问而受到特殊保护的计算机数据的任何人将被认定为犯罪，定罪时，当处以不超过[具体期限]的有期徒刑，或处以数额为[具体数额]的罚款，或二者并罚。

(2) 各国可以针对特定的计算机数据类型来界定犯罪。

第 8 节的条款保护的是已存储或受到保护的计算机数据的机密性。特殊的保护要求对信息的宿主已经实施了保护措施，大大增加了未授权访问数据的难度。具体的实例包括口令和加密。《立法文本解释》指出，有必要使应用于数据或其他财产的保护措施应强于标准的保护措施，例如，限制进入政府大楼的某些部位。[1597]

德国《刑法》

德国《刑法》（版本有效期至 2007 年）第 202a 节也采用了类似的定罪方法。[1598]

第 202a 节— 数据刺探

(1) 未经授权为自己或他人获取不属于他自己而且为防止未授权访问而受到特殊保护的数据的任何人应处以不超过 3 年的有期徒刑或罚金；

(2) 第(1)段中所指的数据系指那些以电磁形式或无法直接看到的形式存储和传输的数据。

这条规定不仅涉及到经济秘密，而且涉及到所有存储在计算机中的数据。[1599] 究其保护的对象而言，这一方法相比于 USC 第 1831 段的经济间谍有所拓展，但这一规定的应用却是受限制的，因为只有在非授权访问受到保护的数据才被认定为是犯罪行为。[1600] 在德国刑法下，对存储在计算机中的数据的保护只限于应采取了措施以避免其成为这类犯罪行为的受害者的个人或公司。[1601]

此类法律条款的相关性

实施这类法律条款应考虑到罪犯授权访问计算机系统（例如，受雇解决一个计算机问题），而此时罪犯滥用其权限而非法获取存储在计算机系统中的数据的情形。[1602]倘若涉及某个权限有权访问计算机系统的情况，那么，通常不可能涉及对非法访问定罪的法律条款。

未获授权

有关数据刺探法律条款的应用通常要求未经受害人许可获取数据。网络欺诈[1603]能够成功实施这一事实清楚地证明基于用户操作的欺诈行为时能成功的。[1604]由于受害人许可，成功操控用户暴露秘密信息的违法者不能按照上述法律条款被起诉。

6.2.4 非法监听

信息通信技术的应用经常伴随着信息安全传输的风险。[1605]不同于传统的国内邮购操作，通过互联网进行的数据传输操作会涉及到很多提供商和数据传输有可能被监听的不同的地点。[1606]监听的最弱点仍在用户，特别是那些没有针对外部攻击采取足够保护措施的个人计算机的用户。由于违法者通常瞄准的最弱点，针对个人用户的攻击是最为严重的，尤其是：

- 易受攻击技术的发展；
- 对违法者而言，个人信息越来越有相关性。

新型网络技术（如，“无线局域网”）为互联网接入提供了诸多益处。[1607]例如，在私人家庭里建立一个无线网络可以使家庭在给定半径范围内的任何地方连接到互联网，无需缆线连接。但是，这项技术的普及和及其带来的便利常常伴随着严重的网络安全风险。如果使用没有受到保护的无线网络，违法者们可以登陆到这个网络实施犯罪活动，无需直接进入住宅。他们只需要进入到无线网络的有效覆盖半径就可以实施攻击。现场测试表面，在某些地区，50%的无线网络没有设置防止未授权监听和访问的保护措施。[1608]在大多数情况下，缺少保护主要是缺少如何设置保护措施的知识。[1609]

过去，违法者主要集中在商业网络实施违法监听。[1610]监听公司的通信信息比监听私有网络中传输的数据更有可能获得有用的信息。个人数据身份盗用数量的增加表明，违法者的攻击重点可能已经发生了变化。[1611]个人数据，如信用卡号、社保号、[1612]口令和银行账户信息现在已经引起了违法者极大的兴趣。[1613]

欧洲理事会《网络犯罪公约》

欧洲理事会《网络犯罪公约》中有一条保护非公共数据传输的条款，该条款认定非授权监听是犯罪行为。这一条款的主要目的在于将电子传输的保护等同于对声音会话的保护，以防止非法分接和/或记录，这类规定目前已存在于大多数立法体制中[1614]。

条款

第 3 条 — 非法监听

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

涉及的违法行为

第 3 条的适用性限于借助技术手段实施的、对传输的监听。[1615] 与电子数据有关的监听可以定义为在传输过程期间获取数据的任何行为。[1616]

如上所述，人们对该规定是否涵盖对储存在硬盘上的信息的非法访问这一问题进行了有争议的诸多讨论。[1617] 总体上，该规定只适用于对传输的监听 — 访问已储存的信息不被认为是对传输的监听。[1618] 事实是，即使在违法者物理接入一个独立计算机系统的情况下，对该条款的适合性的应用也要进行讨论，一部分是由于《网络犯罪公约》没有包含与数据刺探有关的条款，[1619] 而且《公约》的《解释性报告》包含两条针对第 3 条的应用情况、稍显不严密的解释。

《解释性报告》首先指出，该条款涵盖了发生在计算机系统内的通信过程。[1620] 不过，这依然留下一个未解决的问题，即该条款是只应适用于受害者发送数据且随后被违法者截获的情形，还是也应适用于违法者本人操作计算机的情形。第二点与非法获取计算机数据的罪行认定有关。

指南指出，监听者既可以通过使用分接装置间接实施违法行为，也可以“通过访问和使用计算机系统”来实施。[1621] 如果违法者访问计算机系统，并在未授权的情况下用它来拷贝储存于外部磁盘驱动器上的数据，而这种行为导致了数据传输（从内部硬盘向外部硬盘发送数据），那么这一过程不属于监听，而属于由违法者发起的。技术监听缺少的要素是该条款不适用于非法访问储存信息案件的强有力论据。[1622]

“传输”这一术语涵盖所有的数据传输，不论是通过电话、传真、电子邮件，还是通过文件进行的传输。[1623] 第 3 条确定的违法行为仅适用于非公共的传输。[1624] 如果传输过程是机密的，那么传输就是“非公开的”。[1625] 区分公开传输和非公开传输，至关重要的因素不是所传输数据的特性，而是传输过程本身的特性。甚至是传输公共可用的信息，如果涉及传输的各方意在使内容成为其通信秘密，那么也可被视为犯罪。使用公共网络不排除“非公开的”通信。

主观因素

与《网络犯罪公约》定义的所有其他违法行为类似，第 3 条要求违法者是有意地实施了违法行为。[1626] 《网络犯罪公约》没有对“故意”一词作出定义。在《解释性报告》中，起草者指出，对“故意”一词应在国家层面上进行定义。[1627]

未获授权

根据《公约》第 3 条，只有当访问是”未获授权”时，对通信的监听才可被起诉。[1628] 《公约》的起草者提供了一组不属于”未获授权”截获的例子：基于传输各参与者指令或者授权的行为；[1629] 各参与者一致同意的授权测试或保护行为；[1630] 基于刑法规定或者出于国家安全的利益而实施的合法监听。[1631]

在《公约》谈判过程中出现的另一个问题是，信息记录程序的使用是否会导致基于第 3 条的刑事制裁。[1632] 起草者指出，通用的商业惯例（如信息记录程序）不视为未授权的监听。[1633]

限制与保留

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

欧盟有关针对信息系统攻击的指令

欧盟 2013 年有关针对信息系统攻击的指令[1634]第 6 条包含了对非法拦截行为追究刑事责任方面的规定。

> **第 6 条 -** 非法拦截
>
> 成员国应采取必要措施，以确保在未获授权的情况下通过技术手段故意拦截出入某一信息系统或在此系统内部非公开传输的计算机数据（包括从承载此类计算机数据的信息系统发出的电磁辐射）的行为将被追究刑事责任，至少对规模不小的案件应以此等论处。

上述条款的起草遵照了《欧洲理事会网络犯罪公约》所确定的标准[1635]，两者的主要区别体现在对小案件是否定罪的把握上。

《英联邦关于计算机与计算机范围的示范法》

在 2002 年版的《英联邦示范法》的第 8 节中可以找到一种类似的方法。[1636]

> **非法拦截数据等**
>
> 8. 任何人借助技术手段而故意、没有合法或正当理由从事下列活动：
>
> (a) 从计算机系统或在其内部监听任何非公共的传输；或
>
> (b) 监听带有计算数据、来自计算机系统的电磁辐射；即在实施可处罚的违法行为，在定罪时，处以不超过[一定期限]的监禁，或者不超过[一定数量]的罚款，或者两项并罚。

这一条款沿用了类似于欧洲理事会《网络犯罪公约》第 3 条的方法。类似于欧洲理事会《网络犯罪公约》，该条款保护的是非公开传输过程中的数据。

《斯坦福公约草案》

1999 年版的非正式[1637]《斯坦福公约》（草案）（简称“斯坦福草案”）没有明确地对监听计算机数据的行为进行定罪。

6.2.5 数据干扰

国家刑法的一个传统要素是对有形或实质性的对象进行保护，防止其遭到有意破坏。随着数字化进程的继续，更多重要的企业信息作为数据存储起来。[1638] 对这类信息进行攻击或者获取这类信息可造成经济损失。[1639] 除删除外，对此类信息的更改也会造成严重后果。[1640] 过去的法律没有按照对有形对象的保护那样，对数据进行如此彻底的保护。这使得违法者能够设计一些不至于招致刑事制裁的骗局。[1641]

欧洲理事会《网络犯罪公约》

欧洲理事会《网络犯罪公约》第 4 条中有一条用于保护数据完整性免受未授权干扰的规定。[1642] 该规定的目的是弥补某些国家刑法的现有不足，并且为计算机数据和计算机程序提供类似于保护有形对象的保护措施，使之免受有意破坏。[1643]

条款

第 4 条 — 数据干扰

(1) 当未经授权而故意对计算机数据进行毁坏、删除、破坏、更改或限制时，各方应采取必要的法律措施和其他措施，依据本国法律将其认定为犯罪行为。

(2) 签约方可以保留权利，要求将(1)中所述的、导致严重伤害的行为认定为犯罪行为。

涉及的违法行为

第 4 条认定 5 种犯罪行为。“破坏”和“恶化”两个术语系指任何是对数据和程序的信息内容的完整性造成不利改变的任何行为。[1644]“删除”指的是将信息从存储介质中移除的各种行为，并将其视为与销毁有形物体的行为相当。尽管有了定义，但《网络犯罪公约》起草者仍没有区分删除数据的各种不同的方法。[1645] 将文件丢入虚拟的垃圾箱并没有从硬盘中移除该文件。[1646] 甚至“清空”垃圾箱也不一定就能移除该文件。[1647] 因此，目前尚不确定恢复使用已被删除文件是否有碍该条款的应用。[1648]“限制”计算机数据指的是影响介质访问者的数据可用性的行为，在这一行为下，信息以一种不利的方式予以保存。[1649] 针对拒绝服务 [1650] 攻击是否可以应用这一法律条款进行了专门的讨论，[1651] 在这拒绝服务攻击过程中，目标计算机系统上的数据潜在用户和计算机系统的拥有者已经不再可用。[1652]“更改”这一术语指的是现有数据所做的修改，不一定降低数据的可用性。[1653] 这种行为专门涵盖在受害者的计算机上安装恶意软件等行为，如间谍软件、病毒或广告软件等。[1654]

主观因素

与《网络犯罪公约》所定义的所有其他违法行为一样，第 4 条要求违法者故意实施了违法行为。[1655]《网络犯罪公约》没有包含对“故意”一词的定义。在《解释性报告》中起草者指出，“故意”一词应在国家层面上进行定义。[1656]

未获授权

与以上讨论的法律条款类似，违法行为必须是”未获授权”而实施的。[1657] 此前已经讨论过更改数据的权限问题，尤其是在使用“邮件转发器”的情况下。[1658] 邮件转发器用于修改某些数据，目的是为匿名通信提供方便。[1659]《解释性报告》指出，原则上，这些行为被认为是对隐私的一种合法保护，因此，可被视为获得授权后实施的行为。[1660]

限制与保留

第 4 条规定通过将其限于造成严重损害的情况，提供了限制定罪的选择方案，这是一种类似于《欧盟理事会关于信息系统攻击的框架决定》的方法，[1661] 它使各成员国能够限制实体刑法条款对“非未成年人案件”的适用性。[1662]

欧盟有关针对信息系统攻击的指令

欧盟 2013 年有关针对信息系统攻击的指令[1663]第 5 条包含了对非法数据干扰行为追究刑事责任方面的规定。

> **第 5 条** - 数据干扰
>
> 成员国应采取必要措施，以确保在未获授权的情况下故意删除、损坏、恶化、修改或抑制信息系统中的计算机数据或令这些数据无法访问的行为将被追究刑事责任，至少对规模不小的案件应以此等论处。

上述条款的起草遵照了《欧洲理事会网络犯罪公约》所确定的标准[1664]，两者的主要区别体现在对小案件是否定罪的把握上。

英联邦计算机与计算机犯罪示范法

在 2002 年版的《英联邦示范法》第 8 节中可以找到一种与《网络犯罪公约》第 4 条相一致的方法。[1665]

条款内容

> **数据干扰**
>
> 6. (1) 无论何人，没有合法或正当的理由，故意或不计后果地实施了任何一种下列行为：
>
> (a) 破坏或更改数据；或
>
> (b) 使数据变得无意义、无用或无效；或
>
> (c) 阻碍、中断或干扰对数据的合法使用；或
>
> (d) 阻碍、中断或干扰正在合法使用数据的人；或
>
> (e) 拒绝任何有权访问的人访问数据；
>
> 将被认定为实施了一种可处罚的违法行为，在定罪时，处以不超过[具体期限]的监禁，或者不超过[具体数额]的罚金，或者两项并罚。
>
> (2) 无论人们的行为具有临时效应还是具有永久效应，第(1)小节的规定都适用。

第 6 节和《网络犯罪公约》中的对应条款之间的第一个主要区别在于《英联邦示范法》中的条款除认定故意行为属于反作用外，不计后果的行为也属于犯罪行为。与第 6 节不同，示范法中的另外三个条款[1666]（类似于《网络犯罪公约》）限定故意行为属于犯罪行为。将不计后果的行为纳入其中显著拓宽了这种方法的适用性，这样一来，即使是无意从计算机系统中删除文件或破坏存储设备都应受到刑罚处罚。

第二点不同在于第 6 节所涉及的行为与《网络犯罪故意》中的对应条款稍有不同。最终，该条款在第 2 小节中加以说明，即不要求上述行为具有永久效应，即使是临时效应也属于涵盖其中。

《斯坦福公约草案》

1999 年出版的非正式[1667]《斯坦福公约草案》（简称《斯坦福草案》）包含两条对与干扰计算机数据有关的行为进行定罪的条款。

条款

第 3 条

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

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

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

涉及的违法行为

欧洲理事会《网络犯罪公约》和《英联邦示范法》与《斯坦福公约草案》所采用的方法之间的主要区别在于，《斯坦福草案》仅认定干扰了计算机系统运转的数据干扰行为（第 3 条第 1a 段）为犯罪行为，或当所实施行为的目的是提供错误信息以对个人或财产造成损坏时（第 3 条第 1b 段）才对其定罪。因此，《斯坦福草案》没有对删除数据存储设备中普通文本文件的行为进行定罪，原因是这一行为既不会影响计算机的运转，也不会提供错误信息。通过，欧洲理事会《网络犯罪公约》和《英联邦示范法》都遵循了一种更广义的方法保护计算机数据的完整性，且没有进一步的强制性要求。

6.2.6 系统干扰

提供基于信息通信技术服务的个人或企业，依赖其计算机系统的正常运转。[1668] 拒绝服务（DOS）攻击[1669] 使其受害者的网页无法使用，说明了这种攻击的威胁有多么严重。[1670] 此类攻击可以造成巨大的经济损失，并甚至影响到更强大的系统。[1671] 企业并非是这类攻击的唯一目标。全世界的专家目前正在讨论可能出现的专门针对关键基础设施（如，供电系统和电信服务系统等）进行攻击的“网络恐怖主义”。[1672]

欧洲理事会《网络犯罪公约》

为了保护运营商和用户对信息通信技术的使用，《网络犯罪公约》在第 5 条中制定了一条对故意干扰合法使用计算机系统的行为进行定罪的条款。[1673]

条款

第 5 条 — 系统干扰

各方应采取必要的法律措施和其他措施，依据本国法律，将通过输入、传输、破坏、删除、恶化、更改或限制计算机数据，故意在未获授权条件下严重阻碍计算机系统运行的行为判定为犯罪行为。

涉及的违法行为

这一条款的应用要求违法行为阻碍了计算机系统的正常运行。[1674] “阻碍”指的是任何妨碍计算机系统正常运行的行为。[1675] 这一条款的应用限于阻碍是由上述行为之一而实施的阻碍。另外，规定要求“阻碍”行为是“严重的”。各签约国的责任是确定衡量阻碍行为严重性的标准。[1676] 在国家法律框架下，可能存在的限制条件一是“要有最低程度的破坏”二是在对攻击重要计算机系统定罪方面的限度。[1677]

下面所列这些以不利方式影响计算机系统正常运转的行为是确定性。[1678]

“输入”这一术语既不是由《网络犯罪公约》本身定义的，也不是由《网络犯罪公约》的起草者定义的。假如传输是在第 5 条中以一种额外的行为出现，“输入”这一术语可以被定义为任何使用物理输入接口来向计算机系统传输信息的相关行为，而“传送”这一术语涵盖了进行数据远程输入的行为。[1679]

“破坏”和“恶化”这两个术语是有重叠的，在《解释性报告》中，《网络犯罪公约》的起草者针对第 4 条，将其定义为对数据和程序的信息内容信息的完整性作不利修改的行为。[1680]

“删除”这一术语也是由《网络犯罪公约》的起草者相对于第 4 条在《解释性报告》定义的，包括从存储介质中移去信息的行为。[1681]

“更改”这一术语包括对现有数据的修改，不一定降低了数据的可用性。[1682]

“限制”计算机数据是指消极地影响可访问存储信息的介质之人的数据可用性的行为，在这一行为下，信息以一种不利的方式进行保存。[1683]

有关垃圾邮件条款的应用

人们对能否参照第 5 条解决垃圾电子邮件[1684] 问题进行进行了讨论，原因是垃圾邮件可以使计算机系统过载。[1685] 起草者明确声明，垃圾邮件不一定导致“严重”阻碍，而且“对这一行为应当只在通信被故意且严重阻碍的情况下才进行定罪”。[1686]起草者还指出，各方可以根据它们自身的国家法律，采用不同的方法来对阻碍行为进行定罪，[1687] 比如，通过对干扰管理的违法行为进行定罪或者进行制裁。[1688]

主观因素

与欧洲理事会《网络犯罪公约》定义的所有其他违法行为一样，第 5 条要求违法者是故意实施了违法行为。[1689] 这包括故意实施了所列举违法行为之一，以及有严重阻碍计算机系统的正常运转的意图。

《网络犯罪公约》没有包含对“故意”这一术语的定义。在《解释性报告》中起草者指出，“故意”这一术语应在国家层面上进行定义。[1690]

未获授权

违法行为需要是”未获授权”实施的行为。[1691] 如前所述，网络管理员以及负责测试计算机系统保护措施的安全公司担心其工作可能被定罪。[1692] 这些专业人员经计算机系统所有者许可后开展工作，因此是合法行为。此外，《网络犯罪公约》的起草者还明确提出，经所有者授权而对计算机系统的安全性进行测试，不属于“未获授权”。[1693]

限制与保留

与第 2 至 4 条不同，第 5 条不包含在国家法律的实施过程中限制对该条款应用的明确的可能性。尽管如此，各方的责任是确定违法行为的严重程度，这使得它们可能对该条款的应用进行限制。在《欧盟关于信息系统攻击的框架决议》[1694] 中可以找到一种类似的方法。[1695]

《英联邦计算机与计算机相关犯罪示范法》

在 2002 年版的《英联邦示范法》第 7 节中可以找到一种与《网络犯罪公约》第 5 条相一致的方法。[1696]

条款

干扰计算机系统

7．(1) 无论何人，没有合法或正当的理由，有意或不计后果地实施了下列任何一种行为；

(a) 阻碍或干扰了计算机系统的运转；或

(b) 阻碍或干扰了合法使用或操作计算机系统的人；

即在实施一种可处罚的违法行为，在定罪时，处以不超过[具体期限]的监禁，或者不超过[具体数额]的罚金，或者两项并罚。

(1)中，与计算机系统有关的“阻碍”包括但不限于：

(a) 切断计算机系统的电源；以及

(b) 导致对计算机系统的电磁干扰；以及

(c) 通过任何手段使计算机系统恶化；以及

(d) 输入、删除或更改计算机数据；

与《网络犯罪公约》中的对应条款的主要差别在于：根据《英联邦示范法》第 7 节，即使是不计后果的行为也将被定罪，甚至在建设过程中非故意切断电源也会受到刑事制裁。由于有这种规定，所以《示范法》甚至超出了《网络犯罪公约》的要求。另一个差别在于：相比《网络犯罪公约》第 5 条，《英联邦示范法》第 7 节中对“干扰”的定义列出了更多的违法行为。

欧盟有关针对信息系统攻击的指令

欧盟 2013 年有关针对信息系统攻击的指令[1697]第 4 条包含了对非法系统干扰行为追究刑事责任方面的规定。

第 4 条 – 非法系统干扰

各国须采取必要措施，以确保在未获授权的情况下通过输入计算机数据以及通过传输、破坏、删除、恶化、修改或抑制此类数据或令此类数据无法访问而故意严重阻碍或中断信息系统运行的行为将被追究刑事责任，至少对规模不小的案件应以此等论处。

这一条款是基于欧洲理事会《网络犯罪公约》制定的。第一个主要不同在于，除《网络犯罪公约》中规定的行为（输入、传送、破坏、删除、恶化、更改和限制）外，第 4 条将通过导致计算机数据不可访问的方式阻碍信息系统运行的行为也认定为犯罪行为。如果通过非法行为致使数据不可访问，违法者的意图是阻止其他让人访问数据。但是，尽管第 4 条中所列的行为更为复杂，但与《网络犯罪公约》中关于致使不可访问属于限制计算机数据的行为的对应条款在程度上没有区别。对《网络犯罪公约》第 19 版的解释强调，起草《网络犯罪公约》的专家组同意“数据限制”有两个含义：删除数据使其不再物理存在，以及致使数据不可访问。[1698]

《斯坦福国际公约》草案

1999 年版的非正式 [1699]《斯坦福国际公约》草案（“斯坦福草案”）包含了一个对干扰计算机系统的违法行为进行定罪的条款。

条款内容

第 3 条

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

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

涉及的违法行为

《网络犯罪公约》、《英联邦示范法》与《公约》草案方法之间的主要区别在，《斯坦福草案》涵盖任何操纵计算机系统的行为，而欧洲理事会《网络犯罪公约》和《英联邦示范法》仅限于将阻碍计算机系统正常运行的行为认定为犯罪行为。

6.2.7 淫秽或色情资料

非法内容和明显色情内容的定罪及定罪的轻重，国与国之间各不相同。[1700] 参与欧洲理事会《网络犯罪公约》谈判的各签约国着重讨论了关于儿童色情资料的法律协调问题，并排除了对淫秽与色情资料进行更广泛的定罪。有些国家通过执行有关对通过计算机系统进行色情资料交换的行为予以定罪的条款解决了这一问题。不过，由于缺乏标准的定义，因此若违法者是在那些不对色情内容交换行为进行定罪的国家实施其违法行为，将使执法机构难以对这些罪行展开调查。[1701]

实例

对色情资料交换进行定罪的一个例子是德国刑法第 184 节：

第 184 节 — 传播色情作品

(1) 不论是谁，涉及到如下行为（第 11 节第(3)小节）

1. 提供、给予或使 18 岁以下的未成年人能够接触到色情作品；
2. 在 18 岁以下未成年人能够接触到色情作品的场合显示、张贴、展示或以其他方式使未成年人可以获得，或使他们可以看到色情作品；
3. 通过邮购业务或者商业化租赁图书店或读书会的方式，将色情作品出售或给予商业单位以外的零售点、顾客通常不会进入的售货亭或其他销售区域中的另一个人；

3a. 通过商业化出租手段或类似的商业化设施，将色情作品出售或或给予另一个人，以供使用，18 岁以下未成年人不能接触到的和不能看到的商店除外；

4. 通过邮购业务引进色情作品；
5. 在 18 岁以下未成年人能够接触到的或者能够看到的场合公开提供、宣传或评价色情作品，或者通过正常的商业途径在商业交易之外传播色情作品；
6. 在他人未请求这样做的情况下允许另一个人获得色情作品；
7. 为从该放映中得到要求的全部或主要报酬，在公共的电影放映场所中放映色情作品，
8. 制作、获取、供应、储存或引进色情作品，以便在第 1 条至第 7 条规定的情形中使用或拷贝色情作品，或者使另一个人能够实施同样的行为；或
9. 出口色情作品，以便向国外传播色情作品或其复制品，违反该国适用的刑法条款，或者使公众可以接触到色情作品或者使这类行为成为可能，应处以不超过一年的监禁或罚金。

该条款基于这样一种概念：如果没有涉及未成年人，那么对交易和以其他方式交换色情作品，不应予以定罪。[1702] 在此基础上，法律旨在保护未成年人的健康成长。[1703] 接触色情内容是否会对未成年人的健康成长造成负面影响，是一个有争议的话题。[1704] 对在成年人中交换色情作品，根据第 184 节，不会被定罪。“作品”这一术语不仅涵盖传统的作品，而且还涵盖以数字方式存储的作品。[1705] 同样地，“使未成年人可以接触到色情作品”不仅适用于互联网之外的接触方式，而且还涵盖违法者使色情内容在网站上可用的情形。[1706]

这种方法的一个特殊例子是 2007 年版的菲律宾议院第 3777 号法律草案的 4.C.1 节中的条款，该条款对任何色情内容都予以定罪。[1707]

4.C.1： 与网络色情有关的违法行为 — 在不影响依照共和国法案第 9208 号和共和国法案第 7610 号进行的起诉的情况下，无论何人，以任何方式，通过使用信息通信技术，例如但不限于计算机、计算机网络、电视、卫星、移动电话[...]等，宣传、推销网络色情或为网络色情活动提供便利。

第 3i 节： 网络色情或虚拟色情 — 指的是在计算机或通信网络帮助下进行的、任何形式的性行为或性刺激。

本条款沿用了一种非常广泛的方法，原因是它对任何种类的色情广告或者通过互联网进行的宣扬性行为的行为，一概予以定罪。由于双重犯罪原则，[1708] 采用这种广泛方法进行国际调查将会面临诸多困难。[1709]

6.2.8 儿童色情资料

互联网正成为交易和交换包含儿童色情资料的主要手段。[1710] 这种发展趋势的主要原因在于互联网能够快速且有效地传输文件、制作和分发的成本很低，并可以以匿名方式来进行。[1711] 置于网页上的图片可以被世界范围内数以百万计的用户访问和下载。[1712] 提供色情内容或者甚至儿童色情内容的网页之所以如此“成功”，其中一个最重要的原因是互联网用户感到自己很少受到监视，同时可以方便地坐在家里从互联网上下载资料。除非用户利用匿名通信手段，否则他们认为自己是不可能被跟踪的想法是错误的。[1713] 大多数互联网用户不知道他们上网冲浪时会留下电子痕迹。[1714]

用于对儿童色情资料定罪的条款通常用于保护不同的合法利益。对制作儿童色情资料的定罪目的在于保护儿童成为性侵害的受害者。[1715] 在禁止有关儿童色情资料交流（提供、传播）和制作的行为方面，将其认定为犯罪行为的目的在于摧毁这个市场，因为对新作品的不断需求可能会刺激违法者继续侵害海儿童。[1716] 另外，禁止色情作品的交流力图增加人们接触这列作品的难度，进而防止出现对儿童进行性侵害的触发效应。最终，对制作色情作品进行定罪目的是防止违法者使用儿童色情资料引诱儿童从事性行为。[1717]

欧洲理事会《网络犯罪公约》

为了加强和协调对儿童的保护，使其免受性虐待，[1718] 《网络犯罪公约》包括一条旨在解决儿童色情资料问题的条款。

条款内容

第 9 条— 与儿童色情资料有关的犯罪行为

(1) 当未经授权故意实施以下行为时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：

a) 以通过计算机系统分发传播目的而制作儿童色情资料；

b) 通过计算机系统提供儿童色情资料或使儿童色情资料可用；

c) 通过计算机系统传播或传送儿童色情资料；

d) 通过计算机系统为自己或他人购买儿童色情资料；

e) 在计算机系统或计算机数据存储介质中拥有儿童色情资料。

(2) 出于上述第 1 段的目的，“儿童色情资料”这一术语应包括以下视觉描述的色情活动：

a) 未成年人参与直接的性行为；

b) 看起来像未成年人的人参与直接的性行为；

c) 描绘未成年人参与直接性行为的写真图像。

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

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

大多数国家已对虐待儿童以及利用传统方法散播儿童色情资料的行为进行定罪。[1719] 因此，《网络犯罪公约》不限于缩小国家刑法的差距，[1720] – 还力图协调各种不同的规定。[1721]

涉及的违法行为

“制作”这一术语描述的是任何制作儿童色情资料的过程。人们对这一术语进行了不断的讨论。在英国，下载儿童色情图片被视为“制作”儿童色情资料。[1722] 在欧洲理事会《网络犯罪公约》第 9 条中，“购买”和“制作”的差别说明，《公约》的起草者并不认为单纯下载儿童色情资料术语“制作”。然而，虽然《网络犯罪公约》给出了差别，但也需要做进一步的区分。违法者对受侵害的儿童进行拍照术语制作儿童色情资料；但还不能确定一个使用儿童色情照片，并以卡通形式将其放在一起的人是否属于制作儿童色情资料。如果这个人就是卡通作品的作者，即使反映的是一个受侵害的儿童，也不能单纯确定《网络犯罪公约》中“制作”这一术语是否适用。《网络犯罪公约》将制作虚构儿童色情资料的行为（不要求是真实的受侵害儿童）认定为犯罪行为的目的是赞成对“制作”这一数据进行广义解释的一个论据。另一方面，《网络犯罪公约》的《解释性报告》指出，对制作儿童色情资料定罪需要考虑该行为是否属于犯罪的“源头”。[1723] 由于欧洲理事会《网络犯罪公约》并没有明确起草者的意图，所以，《欧洲儿童保护公约》[1724] 的《解释性报告》提供了对类似条款方面更为明确地解释了起草者意图。[1725] 《儿童保护公约》的起草者强调，将制作儿童色情资料认定为犯罪行为对于“对抗性侵害以及挖掘源头是很有必要的”。这可以看做狭义方法支持者的一个论据。

强调基于通过计算机系统传播的目的制作儿童色情资料是必要的。如果违法者制作一个色情作品供自己使用，或者出于非电子传播的目的而制作，那么欧洲理事会《网络犯罪公约》第 9 条就不适用了。针对制作进行讨论的另一个问题涉及自我描写。[1726] 如果违法者设身事外说服一名儿童自己拍摄色情照片，根据国家法律，这将诱使受害者（儿童）犯罪，而非真正的违法者。

“提供”指的是劝说其他人获得儿童色情资料的行为。不必是出于商业目的提供色情资料，但这一术语指的是违法者能够为他人提供色情资料。[1727] “使可用”指的是能够使其他使用者接触到儿童色情资料的行为。这一行为因其将儿童色情资料置于网页或链接到文件共享系统，并能使其他人接触到这类存放在未设防的存储器或文件夹下的资料。

“传播”是指向其他人转发儿童色情资料的行为。“传送”指的是利用所传输的信号进行的一切通信活动。为自己或为他人“购买”指的是任何积极获取儿童色情资料的行为。

第 9 条最后将“拥有”儿童色情资料也视为犯罪行为。对拥有儿童色情资料进行定罪也与国家法律制度不同。[1728] 对这类作品需求导致儿童色情资料的不断制作。[1729] 拥有这类作品会刺激对儿童的性侵害，所以，起草者建议，抑制儿童色情资料制作的一条有效途径是将拥有儿童色情资料视为违法行为。[1730] 但在第 4 段中，通过限制制作、提供、传播儿童色情资料的刑事责任，《公约》允许各方将拥有除外。[1731] “拥有”这一术语涉及故意接触儿童色情资料的人的控制行为。它要求违法者有控制行为，这一行为不仅涉及本地存储设备，而且涉及到他可以访问和控制的远程存储设备。此外，“拥有”这一术语一般要求有上述定义中所说的主观因素。

儿童色情资料

第 9 条第 2 段专门针对儿童色情活动视觉描绘的作品给出了三个小节：未成年人从事直接的性行为；看起来像未成年人的人从事直接的性行为；展示未成年人从事直接性行为的写真图像。这种情况要求有“视觉描绘”，不包括声音文件。

即使起草者力图改善儿童对性侵害的保护措施，第 2 段中所涉及的合法权益也是广义上的。第 2(a)段直接针对儿童侵害。第 2(b)段和 2(c)段涉及到未侵害儿童权益的图像，如通过使用 3D 建模软件制作的图像。[1732]将虚构儿童色情资料认定为犯罪行为的原因是，这些图像能够用于引诱儿童参与到类似的色情活动中，不一定对真实的儿童造成伤害。[1733]

该定义将重点放在视觉描绘上是其面临的主要问题。儿童色情资料不一定以图片或视频的形式传播，还可以是声音文件。[1734] 由于第 9 条给出的条款指的是针对儿童的“视觉描绘资料”，并不包括声音文件。因此，很多当前的立法，例如《HIPCAR [1735] 网络犯罪立法文本》[1736] 采用了不同的描述途径，以避免出现“视觉”这一术语。

定义

3.

[…]

(4) 儿童色情资料系指直接展现或描述下列色情内容的作品：

a) 儿童从事直接的性行为；

b) 看起来像儿童的人从事直接的性行为；或

c) 描绘儿童从事直接性行为的图像；

这些行为包括但不限于音频、视频或文本型申请作品。

各国可以通过不执行(b)款和(c)款来限制对上述行为的定罪。

《买卖儿童、儿童卖淫和儿童色情中的儿童权益公约任择议定书》第 2 条 c)款给出了另一个更宽泛的定义。

第 2 条

出于本任择议定书的目的：

[…]

(c) 儿童色情资料系指通过任何方式任何展示儿童从事真实的或虚拟的直接性行为，或者出于性目的展示儿童性器官的作品。

与国家法律的一个最重要的不同在于所涉及人员的年龄。某些国家在其国家法律中定义对与儿童色情去有关的术语“未成年人”的定义与《欧盟儿童权益公约》[1737] 第 1 条 “儿童”的定义相符，即均指所有年龄小于 18 岁的人。其他国家将未成年人定义为 14 岁以下的人。[1738] 在 2003 年颁布的《欧盟委员会关于反对儿童性侵害和儿童色情资料框架决议》[1739] 和 2007 年颁布的《欧洲理事会关于保护儿童免受性侵犯与性虐待公约》[1740] 可以找到类似的方法。在强调年龄与国际标准一致的重要性的前提下，《网络犯罪公约》根据《欧盟公约》定义了这一术语。[1741] 然而，考虑到与现有国家法律的巨大差别，《网络犯罪公约》允许各国要求有不同的年龄限制，但不得小于 16 岁。一个争论越来越频繁的问题是，如果所定义的允许从事性行为的年龄与定义规定的年龄限制不同，那么就有可能存在的非故意犯罪。[1742] 例如，如果将儿童色情资料定义为 18 岁以下之人性行为的直接描述，而允许从事性行为的年龄是 16 岁，则两名 17 岁的儿童可以合法地发生性关系，在这种情况下，如果这两名儿童对其性行为进行拍照或录像，则他们可能被判犯有严重罪行（制作儿童色情资料）。[1743]

主观因素

与欧洲理事会《网络犯罪公约》确定的所有其他违法行为一样，第 9 条要求违法者故意实施了违法行为。[1744] 在《解释性报告》中，起草者明确指出，《网络犯罪公约》不对无意中接触到儿童色情资料的行为进行定罪。“无意”专指以下情况，即罪犯偶然打开了一个带有儿童色情图像的网页，并且尽管他立即关闭了网站，但有些图片也已保存在了临时文件夹或缓冲文件中。

未获授权

根据《网络犯罪公约》第 9 条的规定，只有违法者在“未获授权”的情况实施与儿童色情活动有关的行为时采会被起诉。[1745] 《网络犯罪公约》起草者没有进一步规定在哪些情况下用户的行为是经授权的行为。一般只有在调查犯罪案件过程中，执法机构的人员浏览儿童色情内容的行为才不属于“未获授权”。

《欧洲儿童保护公约》

《欧洲理事会关于保护儿童免受性侵犯与性虐待公约》第 20 条是对与儿童色情有关的行为进行定罪的另一方法。[1746]

条款

第 20 条– 涉及儿童色情资料的违法行为

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

a) 制作儿童色情资料；

b) 提供儿童色情资料或使之可用；

c) 散布或传输儿童色情资料；

d) 为自己或为他人获取儿童色情资料；

e) 拥有儿童色情资料；

f) 明知通过信息通信技术可访问到儿童色情资料而去访问。

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

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

– 排他地包含模拟的展示或者非实际存在儿童的真实图像；

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

(4) 各方可以全部或部分保留不应用第 1.f 段的权利。

涉及的违法行为

这一条款的依据是欧洲理事会《网络犯罪公约》中的第 9 条，因此，在很大程度上与这一条款相当。[1747] 主要的区别在于《网络犯罪公约》着眼于对与信息通信服务有关的行为进行定罪（“出于通过计算机系统散布的目的而制作儿童色情资料”），同时，《保护儿童公约》主要遵循一种更广义的方法（“制作儿童色情资料”），甚至涵盖了那些与计算机网络无关的行为。

尽管在所涵盖的违法行为方面存在相似之处，《保护儿童公约》第 20 条仍包含了一种《公约》未涵盖的行为。根据《保护儿童公约》第 20 条第 1f 段，将对通过计算机访问儿童色情资料的行为进行定罪。这使执法机构能够在证明违法者打开过带有儿童色情内容的网站、但无法证明违法者下载过这些资料的情况下，对违法者进行起诉。在收集证据方面存在此类困难，例如，如果违法

者对其存储介质中受保护的下载文件使用加密技术，那么就会造成难以收集证据。[1748]《保护儿童公约》的《解释性报告》指出，对违法者只是在线观看了儿童色情图片而没有下载的情形，该条款也应适用。[1749] 一般地，打开一个网站会自动启动下载过程 — 通常是在用户不知情的情况下。[1750] 因此，《解释性报告》中提到的情形只与以下情形有关，即未进行后台下载。这一条款也适用于不通过下载而使用儿童色情资料的案件。例如，如果网站使用流视频则不需要下载，流过程的技术配置可以使接收信息时不需要缓冲，而是在传送完成后直接丢弃。（例如，如果违法者使用视频流）。

英联邦计算机和计算机相关犯罪示范法

在 2002 年版的《英联邦示范法》第 10 节有一种与欧洲理事会《网络犯罪公约》第 9 条相一致的方法。[1751]

儿童色情资料

10.

(1) 故意实施下列行为的人:

(a) 通过计算机系统发布儿童色情资料；或

(b) 出于通过计算机系统发布的目的制作儿童色情资料；或

(c) 在计算机系统或计算机数据存储介质中拥有儿童色情资料；

犯有可处罚的罪行；定罪时，可出以不超过[具体期限]的监禁，或处以不超过[具体数额]的罚金，或二者并罚。[1752]

(2) 如果一个人出于纯科学研究、医学或执法的目的制作儿童色情资料，则不属于(1) (a)或(1)(c)规定的犯罪行为。[1753]

(3) 在这一节中，“儿童色情资料”是含有视觉上描绘下列行为的作品:

(a) 未成年人从事直接的性行为；或

(b) 看起来像未成年人的人从事直接的性行为；或

(c) 展示未成年人从事直接性行为的图像。

“未成年人”指的是年龄小于[X]岁的人。

“发布包括”:

(a) 分发、传送、散布、传播、递送、展示、出租、交换、交易、销售或供销、出租或供应出租、以任何方式提供、或以任何方式使其可用；或

(b) 以从事 (a) 中所列行为为目的，拥有或保管或控制；或

(c) 以从事 (a) 中所列行为为目的，以任何其他方式打印、影印、复制或制作（不论类型和性质是否相同）。

与《欧洲网络犯罪公约》的主要不同在于，《英联邦示范法》没有对“未成年人”这一术语给出确定的定义，它允许各成员国确定年龄界限。与欧洲理事会《网络犯罪公约》类似的是，《英联邦示范法》没有给出针对以信息技术方获得儿童色情资料的情形定罪的条款。

《欧盟儿童权益公约任择议定书》

针对买卖儿童、儿童卖淫和儿童色情资料的任择议定书》第 3 条给出了一种技术上处于中性的方法。

> **第 3 条**
> 1 各国应至少确保其刑法中涵盖所有下列活动或行为，不论这些违法行为在国内或国家之间对个人或组织如何定罪：
> [...]
> (c) 出于上述目的制作、分发、散布、进口、出口、供应、销售或拥有第 2 条所定义的儿童色情资料。
> [...]

虽然《任择议定书》明确规定传播这类儿童色情资料的媒介为互联网，[1754] 但该议定书仍以技术上中性的方法来对有关儿童色情资料的行为进行定罪。儿童色情资料被定义为：不论以何种方式展示儿童从事真实的或虚拟的直接性行为，或主要出于性目的展示儿童性器官的任何行为。[1755] 所涉及的行为与《网络犯罪公约》中所涉及的行为相当，所不同的是第 3 条中的规定仍属于技术中性的。

《斯坦福国际公约》草案

1999 年出版的非正式[1756]《斯坦福国际公约》（草案）（简称“斯坦福草案”）没有包含任何针对通过计算机系统交换儿童色情资料行为定罪的条款。《斯坦福草案》的起草者指出，通常情况下，根据《斯坦福公约》草案，没有哪种类型的言论或出版物要求被视为犯罪行为。[1757] 认识到这些不同的国家方法后，《斯坦福草案》的起草者将其留给各成员国来决定对这方面的定罪。[1758]

6.2.9 教唆儿童

互联网能够使人们在不显露年龄和性别的情况下进行沟通。这种能力可以被违法用来教唆儿童。[1759] 这种现象通常称作“培养”。[1760] 有些地区性法律框架包含针对这种联系方式进行定罪的条款。

《欧洲理事会儿童保护公约》

《欧洲理事会关于保护儿童免受性侵犯与性虐待公约》第 23 条是上述条款的一个例子。[1761]

> **第 23 条 – 出于性目的教唆儿童**
> 各方应制定必要的法律或采取必要的措施，对下述行为定罪，即如果成年人借助 ICT 主动提议约见未满第 18 条第 2 款所规定年龄的儿童，目的在于针对他或她实施 18 条第 1 款或第 20 条 1.a 所列的任何一种犯罪行为，不论违法者的提议是否已经构成实质性的约见行为。

出于性虐待的目的教唆儿童的行为没有包含在针对儿童性虐待定罪的条款中，在这种情况下，“教唆”被视为预备行为。由于针对网上培养问题存在越来越大的争论，所以，《公约》起草者决定将第 23 条包含其中，用以对已经实施的预备行为进行定罪。[1762] 为避免量刑过重，《公约》的起草者强调，与儿童进行单纯的性聊天不应被视作足以定罪的教唆行为，尽管这可能是性虐待预备工作的一部分。[1763]

这种立法方法存在两个主要问题。首先，该条款只涉及通过信息通信技术进行教唆，没有包括其他形式的教唆。起草者表示，将重点放在这类技术上是很合理的，因为这类技术不好监控。[1764] 然而，还没有足够的可靠数据来证明儿童教唆仅仅是一个网络问题。另外有很好的理由，不仅可以避免出现类似的情况 — 在线上实施是非法的，而在线下实施就是合法的，相反，可以确保合法离线时的线上行为不受到刑事制裁。例如，《针对新世纪言论自由问题的联合声明》（2001）指出，各个国家不应采取隔离从事来限制互联网的内容。[1765]

对这种预备行为进行定罪的另一个问题则是有可能与刑法体制发生冲突，因而有可能没有将非常严重行为的犯罪预备包含其中。如果是儿童性虐待犯罪准备是有罪的，而谋杀儿童的犯罪预备则不受处罚，这将挑战一个国家的价值体系。因此，任何这类方法都应针对将预备行为定罪的优点和风险进行全面的讨论。

6.2.10 仇恨言论、种族主义

对仇恨言论的定罪程度存在着显著的差异。[1766] 特别是在一些宪法保护言论自由的国家，[1767] 仇恨言论通常不被定罪。禁止仇恨言论主要集中在非洲和欧洲。[1768]

欧洲理事会《网络犯罪公约》（附加协议）

欧洲理事会在反对种族主义方面发挥着非常重要的作用，维也纳峰会后，1993 年批准通过了《反对种族主义、排外主义、反犹太主义和种族偏见的声明和行动计划》。[1769] 1995 年，欧洲理事会通过了《与种族主义作斗争的建议》。[1770] 在欧洲理事会《网络犯罪公约》的谈判过程中，对网络仇恨言论和种族主义的定罪问题进行了讨论。由于参与讨论《网络犯罪公约》的各国不能对仇恨言论和排外资料定罪达成一致。[1771] 有关这类犯罪行为的条款集中整合到独立的《公约第一议定书》中[1772]。对排外主义言论定罪的条款面临的主要问题之一是，一方面要保证言论自由[1773]，另一方面还要保护个人和集体的利益不受到侵害。毋庸细说，欧洲理事会《网络犯罪公约》[1774] 谈判过程中以及《附加议定书》[1775] 的签字认可的状态时存在的困难说明，对言论自由保护程度的不同成为统一进程的一大障碍[1776]。特别是对于双重犯罪 [1777] 的通用原则，由于缺少协调，结果使法律条款在国家之间的案件中应用时出现了困难。[1778]

条款

第 3 条—通过计算机系统散布种族主义和排外主义资料

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

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

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

第 4 条—因种族主义和排外主义而造成的威胁

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

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

第 5 条— 因种族主义和排外主义而造成的侮辱

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

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

2. 签约方或者：

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

b. 全部或部分保留不运用本条款第 1 段的权利。

第 6 条— 否认、完全低估、赞成种族灭绝或反人类罪行，或者为其辩护

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

通过计算机系统向公众散播或为公众提供某些否定、完全低估、赞成种族灭绝或反人类罪行或为其辩护的资料认定为犯罪行为。（种族灭绝或反人类罪行由国际法定义，并被依照 1945 年 8 月 8 日的《伦敦协定》建立的国际军事法庭出具的有最终具有约束力的决议认可，或被依照相关国际文件建立且其审判权被各方认可的任何其他国际法庭的最终具有约束力决议认可。）

2. 一方或者：

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

b. 全部或部分保留不应用本条款第 1 段的权利。

涉及的违法行为

第 3 条将故意通过计算机系统向公众散播和提供排外主义资料确定为犯罪行为。[1779] 因此，没有涉及不包括计算机系统在内的传统出散播途径（如书本和杂志）。根据第 2 条给出的定义，种族主义和排外资料指的是：以种族、肤色、血统或国家或种族起源以及宗教为由，针对任何个人或团体鼓吹、宣传或煽动仇恨、种族歧视或暴力的任何书面资料、图像或其他观点和理论的表述载体。散播指的是上述资料的散布活动。[1780]“提供”指的是将这些资料置于网上的行为。[1781] 他要求使用者能够获得这些资料。实施这些行为可以通过将资料置于网站或连接到文件共享系统，并使其他人能在未受限存储单元或文件夹中获得这类资料来实施。《解释性报告》指出，建立或编辑超链接也属于此类违法行为。[1782] 因为超链接只是方便获得这些资料，这样的解释超出了条款文本中的定义。散播这一术语涉及向其他人转发种族主义或排外主义资料的行为。定罪时，要求是向公众散播和提供这类资料，而非私人通信。[1783]

第 6 条沿用了第 3 条的方法，将通过计算机系统向公众 [1784] 散播或为公众提供某些否定、完全低估、赞成种族灭绝或反人类罪行或为其辩护的资料认定为犯罪行为。（种族灭绝或反人类罪行由国际法定义，并被依照 1945 年 8 月 8 日的《伦敦协定》建立的国际军事法庭出具的有最终具有约束力的决议认可，或被依照相关国际文件建立且其审判权被各方认可的任何其他国际法庭的最终具有约束力决议认可。）

第 4 条将通过计算机系统，利用严重刑事犯罪来恐吓他人，其原因是被恐吓对象属于可以用种族、肤色、种族、血统或国家或种族起源以及地区来区分的另一组群，或者是可以用上述特征之一区分的一群人。它指的是能够造成那些认为有可能受到犯罪侵害的人群中造成恐慌。[1785] 不同于第 3 条，“威胁”这一术语不要求有任何与公众的交流，因此也包括向受害人发送电子邮件。

第 5 条采用了与第 4 条类似的方法，将辱骂他人认定为犯罪行为，其原因是被辱骂对象属于可以用种族、肤色、种族、血统或国家或种族起源以及地区来区分的另一组群，或者是可以用上述特征之一区分的一群人。“辱骂”指的是损害他人尊严的任何冒犯性的或攻击性的表述，辱骂的内容直接与被褥骂人所属的群体有关。为了避免与言论自由[1786] 的原则发生冲突，有必要从狭义上定义这种侮辱行为。第 4 条和第 5 条的主要区别在于，该条款只要求公开辱骂，因此不包括私人通信（例如电子邮件）。[1787]

《斯坦福国际公约》草案

1999 年出版的非正式 [1788]《斯坦福国际公约》草案（简称“斯坦福草案”）不包括对仇恨言论定罪的条款。《斯坦福草案》的起草者指出，在《斯坦福草案》下，没有那种类型的言论或出版物被视作犯罪。[1789] 认识到这些不同的国家方法后，《斯坦福草案》的起草者将其留给各成员国来决定对这方面的定罪。[1790]

6.2.11 宗教犯罪

国与国之间对宗教信仰及其符号的保护强度存在着差异。[1791] 更多的差异表现在罪行认定上。2006 年的《联合国意见与表达自由特殊报告员、OSCE 媒体自由代表和 OAS 自由表达特殊报告员联合声明》中指出，在“很多国家，这各领域过于宽泛的规则被当权者滥用作限制非传统的、不同意见、批评的或少数人的声音，或讨论挑战性的社会问题”。[1792] 2008 年的联合声明强调，国际组织，包括联合国大会和人权理事会应抵制进一步采纳支持对宗教诽谤定罪观点的声明。

欧洲理事会《网络犯罪公约》（附加协议）

在《网络犯罪公约》各方对这一主题谈判的过程中，面临着与排外主义资料中所发现的相同困难。[1793] 尽管这样，参与《网络犯罪公约》《第一附加议定书》条款谈判的各国，同意在两个条款中将宗教内容增加为保护对象。

条款

第 4 条— 以种族和排外为动机的恐吓

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

通过计算机系统，以实施其国内法律所定义的严重犯罪行为为由，以其种族、肤色、种族、血统或国家或种族起源以及地区为借口恐吓(i)以这些特征来区分的另一组群中的人；(ii)带有这些特征中任何一种特征的群体。

第 5 条— 以种族和排外为动机的侮辱

1. 当以下行为是未经授权而故意进行时，各方应采取必要的法律措施和其他措施，依据本国法律将其判定为犯罪行为：通过计算机系统，以其种族、肤色、种族、血统或国家或种族起源以及地区为借口公开侮辱(i)用这些特征来区分的另一群体中的人；(ii)带有这些特征中任何一种特征的群体。

[…]

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

国家立法实例：

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

295-B. 玷污《古兰经》：无论何人，恶意地玷污、破坏或亵渎《古兰经》的副本或是从中摘录的文字，或者以任何不敬的方式使用它，或者出于任何非法目的，应处以终身监禁。

295-C. 对“先知”使用不敬的言论等：无论何人，使用口头或书面语言，或者通过可视的展示，或者通过直接或间接地诋毁、影射、暗讽或玷污先知穆罕默德的神圣名字（他身边和平的力量），应处以死刑或终身监禁，还应处以罚款。

至于这一条款应用的不确定性，2006 年版的《巴基斯坦电子犯罪法案》草案包含了两条着重于与互联网有关的违法行为 [1794] 的条款。但当法案 2007 年被重新提出作为《电子犯罪公约》这些条款都被删减了，[1795] 该公约 2007 年 12 月公布。[1796]

20. 亵渎《古兰经》副本等 — 无论何人，使用任何电子系统或电子设备，恶意地玷污、破坏或亵渎《古兰经》的副本或是从中摘录的文字，或者以任何不敬的方式使用它，或者出于任何非法目的，应处以终身监禁。

21. 对“先知”使用不敬的言论等 — 无论何人，使用任何电子系统或电子设备，使用口头或书面语言，或者通过视觉的展示，或者通过直接或间接地诋毁、影射、暗讽或玷污先知穆罕默德的神圣名字（他身边和平的力量），应处以死刑或终身监禁，还应处以罚款。

与关于对利用互联网散布排外主义资料的行为进行定罪的条款一样，全球方法面临的主要问题之一是对宗教违法行为进行定罪涉及言论自由原则。[1797] 正如之前所指出的那样，对言论自由不同的保护程度阻碍了法律协调过程。[1798] 尤其是对双重犯罪通用原则，[1799] 法律协调的缺失将会给具有国际影响的案件的执行带来诸多困难。[1800]

6.2.12 非法赌博

越来越多的网站提供非法赌博，这已成为一个令人关注的问题，[1801] 原因是它们可以用来绕过某些国家中强制执行的赌博禁令。[1802] 如果服务是在不禁止在线赌博的国家中进行操作的，那么各国将难以对互联网赌博的运营进行定罪，以阻止其国民使用这些服务。[1803]

国家立法实例

《网络犯罪公约》没有包含禁止在线赌博的条款。在这方面，德国《刑法》第 284 节给出了国家方法的一个实例：

实例

第 284 节 — 未授权组织赌博游戏

(1) 无论何人，未获得公共机关的许可，公开组织或经营一种赌博游戏，或者使这种设备可用，应处以不超过两年的监禁或一定数量的罚款。

(2) 定期在俱乐部或私人派对中进行的赌博游戏，应视为是公开组织的赌博活动。

(3) 无论何人，在第(1)小节所述的案件中，其行为：

1. 是专业的；或者
2. 作为团伙的一员，而该团伙是为了持续实施此类行为而组织起来的，应处以三个月到五年的监禁。

(4) 无论何人，为公开赌博游戏招募人员（第(1)小节和第(2)小节），应处以不超过一年的监禁或一定数量的罚款。

该条款通过定义组织赌博游戏的过程，旨在限制赌博成瘾 [1804] 的风险。[1805] 该条款没有明确集中于与互联网有关的赌博游戏，但包括对赌博游戏的定义。[1806] 在这方面，将未获得公共机关的许可而开展的非法赌博活动认定为犯罪行为。另外，该条款还将故意提供赌博工具，并将其用于非法赌博的人犯有罪行。[1807] 由于违法者将面临更高的刑法，所以这种定罪方法远远超出了援助与支持的结果。[1808]

为了避免招致犯罪调查，非法赌博网站的经营者可以物理地将其行为 [1809] 转移到那些不对非法赌博定罪的国家。[1810] 此类地点转移对执法机构而言是一项挑战，原因是服务器位于其所在国的管

辖范围之外，[1811] 通常不会影响到国内的用户访问它。[1812] 为了提高执法机构与非法赌博作斗争的可能性，德国政府将定罪范为扩大至用户。[1813] 根据第 285 节，执法机构可以起诉参与非法赌博的用户，并且可以启动调查，即使赌博游戏的运营者身处德国之外，无法对他们进行起诉：

第 285 节 — 参与未授权的赌博游戏

任何参与聚众赌博游戏（第 284）的人应处以不超过 6 个月的监禁和每天 180 美元的罚款。

如果违法者使用赌博网站进行洗钱活动，那么识别这样的违法者是很难的。[1814] 用来防止非法赌博立法 [1815] 的一个具体实例是 2005 年的美国非法网络赌博法案。[1816]

第 5363 段. 禁止接受任何用于非法互联网赌博的金融手段

任何从事博彩业的人都不得有意接受与任何参与非法互联网赌博之人有关的

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

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

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

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

第 5364 段. 识别和防止受限业务的政策与程序

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

(1) 建立一些政策和程序，它们

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

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

(2) 建立一些政策和程序，以防止接受支付系统中与受限业务有关的产品和服务。

(b) 在依据第（a）小节规定制度时，财政部长将：

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

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

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

(c) 金融业务提供商将被认为是符合第（a）小节中所规定的制度的，如果：

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

(A) 识别和阻拦受限业务；或者

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

以及

(2) 指定之支付系统的此类政策和程序符合第（a）小节所规定之制度的要求。

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

(1) 这是一项受限业务；

(2) 此人合理地认为这是一项受限业务；或者

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

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

第 5366 段. 刑事处罚

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

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

该法案的目的是为了应对互联网赌博的挑战和（跨境）威胁。[1817] 它包含两个重要的规定：首先，禁止接受任何从事博彩业之人用于非法互联网赌博的任何金融工具。这一条款没有管制由互联网赌博网站或金融机构的用户所实施的行为。[1818] 违反这一禁令可招致刑事制裁。[1819] 此外，该法案要求财政部长和美国联邦储备系统监管理事会规定一些制度，要求金融业务提供商通过合理的政策和程序，识别和阻拦与非法互联网赌博有关的受限业务。第二条规定不仅影响从事博彩也的人，而且一般会影响所有的金融机构。与接受从事博彩业之人用于非法互联网赌博的金融工具不同，金融机构一般不会面临刑事责任。至于可能与《服务贸易总协定》（GATS）[1820] 有冲突的规定的国际影响问题，目前正在研究中。[1821]

6.2.13 侮辱与诽谤

诽谤和公开发表虚假信息并非只是能在网络中实施的违法行为。但正如之前所指出的那样，匿名通信的可能性 [1822] 以及与互联网中大量可用信息有关的逻辑挑战 [1823]，都是支持此类违法行为的抽象要素。

是否要求对诽谤进行定罪是一个有争议问题。[1824] 对诽谤进行定罪应首先考虑与“言论自由”原则可能发生冲突的因素。因此，大量的组织呼吁替换关于诽谤的刑法条款。[1825] 联合国观点和言论自由问题特别报告人以及 OSCE 媒体自由代表表示：

尽管有这些考虑，但一些国家 [1826] 已经实施了对诽谤进行定罪的刑法条款，同时也对虚假信息的公开发布予以定罪。重要的是强调，即使在那些对诽谤予以定罪的国家内，案件的数量也极不相同。在英国，2004 年全年没有人因诽谤而遭起诉，2005 年也只有一个嫌疑人因诽谤而遭起诉。[1827] 德国的犯罪数据统计记录，2006 年有 187 527 件诽谤案件。[1828] 《网络犯罪公约》、《英联邦示范法》和《斯坦福草案》没有包含直接涉及这些行为的条款。

国家法律实例

涉及诽谤的刑法条款的一个例子是《昆士兰刑法》（澳大利亚）中的第 365 节。通过 2002 年版的《2000 年刑法诽谤修正案法案》，昆士兰重新引入了有关诽谤的刑法责任。[1829]

条款

365 违法诽谤 [1830]

(1) 无论何人，没有合法理由，公开发表诽谤他人（相关人员）的内容 —

(a) 明知该内容是虚假的，或者没有注意到内容究竟是真的还是虚的；以及

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

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

另一个对诽谤进行定罪的例子是德国《刑法》第 185 节：

条款

第 185 节 — 侮辱

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

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

6.2.14 垃圾邮件

在所有的电子邮件中，多达 75% [1831] 的电子邮件被报告为垃圾电子邮件，[1832] 对是否需要对垃圾电子邮件进行刑事制裁进行了激烈讨论。[1833] 用于解决垃圾邮件问题的国家法律解决方案各不相同。[1834] 垃圾邮件为什么仍然是一个问题？其中一个主要原因是，过滤技术仍无法识别和阻拦所有的垃圾电子邮件。[1835] 保护措施仅仅针对主动发送的电子邮件提供了有限的保护措施。

2005 年，OECD 发布了一份报告，分析了垃圾邮件对发展中国家的影响。[1836] 报告指出，来自发展中国家的代表常常表达这样的观点，即他们国家的互联网用户正受到越来越严重的、来自垃圾邮件和网络滥用的影响。对报告的结果进行分析可以证明，代表们的看法是正确的。由于资源更为有限、更为昂贵，与西方发达国家相比，发展中国家的垃圾邮件问题明显要严重的多。[1837]

不过，不仅仅在识别垃圾邮件方面存在很多困难。在接收者不期望收到、但合法发送的电子邮件与那些非法发送的电子邮件之间进行区分，也是一个问题。当前基于计算机传输（包括电子邮件和 VoIP）的发展趋势，突显了保护通信不受攻击的重要性。如果垃圾邮件超过一定的级别，那么它们可能严重阻碍对信息通信技术的应用，并降低用户的效率。

欧洲理事会《网络犯罪公约》

欧洲理事会《网络犯罪公约》没有明确对垃圾邮件予以定罪。[1838] 起草者建议，对这些行为的定罪应限于严重和有意阻碍通信的行为。[1839] 这一方法没有将重点放在非请求的电子邮件上，而是着重于垃圾邮件对计算机系统或网络的影响。基于《网络犯罪公约》的法律方法，与垃圾邮件作斗争可能只能基于对计算机网络和系统的非法干扰：

第 5 条— 系统干扰

各方应采取必要的法律措施和其他措施，依据本国法律将利用输入、传递、破坏、删除、毁坏、更改或限制计算机数据等手段，未经授权故意严重阻碍计算机系统的正常运转的行为判定为犯罪行为。

《斯坦福国际公约》草案

1999 年出版的非正式[1840] 《斯坦福草案》没有包括对垃圾邮件进行定罪的条款。与《网络犯罪公约》一样，《斯坦福公约》草案只对有意造成目标系统干扰的垃圾邮件违法行为进行定罪。

《HIPCAR 网络犯罪立法文本》

《HIPCAR [1841] 网络犯罪立法文本》第 15 节给出了这种特殊方法的一个具体实例：[1842]

垃圾信息

15. (1) 任何人，如果没有合法借口或理由，故意从事下列行为或过多利用合法借口或理由：

(a)故意从计算机系统或通过该计算机系统发起多封电子邮件消息的传送；或

(b) 出于欺骗或误导用户、邮件或互联网服务提供商的目的，使用受保护的计算机系统转发或中继多封电子邮件，造成邮件消息来自这些计算机系统的假象；或

(c) 在多个电子邮件消息中实质性地伪造头信息并发送这些邮件消息将被判有罪，定罪时，应处以不超过[具体期限]的监禁，或不超过[具体数额]的罚金，或二者并罚。

(2) 各国可以将发送多封电子邮件消息行为的定罪范围限制在顾客之间或商业伙伴之间的邮件传送。如果有更有效的补充措施，各国可以自行决定对 15 (1) (a)中所规定的行为不予定罪。

这一条款包括三种不同的行为。第 15 节 (1) (a) 涉及发起多封电子邮件的发送。第 3 节(14)定义了作为邮件消息发送给成千上万收件人的多封电子邮件。在这种过去看下，《附注》中指出，将这类行为的定罪限定为没有合法借口或理由前提下实施对于区分合法群发邮件（类似于新闻稿）和非法垃圾邮件具有很重要的作用。[1843] 第 15 节 (1) (b)将利用滥用受保护的计算机来转发或传送电子消息，从而避开防垃圾邮件技术的行为认定为犯罪行为。第 15 节 (1) (c)涉及对利用伪造头信息来避开防垃圾邮件技术的行为的定罪问题。《附注》强调，第 15 节要求违法者是在没有合法借口或理由的情况下故意实施违法行为。[1844]

美国法典

这限制了在以下案件中对垃圾邮件的定罪，即垃圾电子邮件的数量对计算机系统的处理能力产生了严重影响。对影响商务有效性、但不一定影响计算机系统的垃圾电子邮件，可能不会被起诉。因此，许多国家采用一种不同的方法。一个例子是美国法典 – 18 USC § 1037。[1845]

§ 1037. 与电子邮件有关的欺诈和相关行为

(a) 一般情况 — 无论何人，从事或影响到国与国之间的贸易或者对外贸易，明知 —

(1) 未获授权而访问一台受保护的计算机，并且从该台计算机或者通过该台计算机，故意意发送多封商务电子邮件消息；

(2) 使用一台受保护的计算机转发或重发多封商务电子邮件消息或互联网接入服务，目的在于欺骗或误导邮件接收者，造成这台计算机是此类消息的源头的假象；

(3) 对多封商务电子邮件消息中的头信息做实质性修改，并故意传送此类消息，

(4) 使用经对实际注册者身份进行实质性篡改后的信息来注册五个或更多个的电子邮件账号或者在线用户账号或者两个或更多个域名，并且有意地用此类账号或域名的某种组合来传送多份商务电子邮件消息，或者

(5) 虚假地将自己介绍为注册者或者 5 个或更多个互联网协议地址注册者权益的合法继承者，并且有意第从此类地址传送多份商务电子邮件消息，

或者密谋这样做，将被处以第（b）小节所规定的处罚。

(b) 处罚 — 依据第（a）小节，对违法行为的处罚是：

(1) 一定数量的罚款，或者不超过 5 年的监禁，或者两项并罚，如果 —

(A) 根据美国或任何州的法律，这些违法行为的实施促进了任何重罪；或者

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

这一条款由 2003 年版的《CAN 垃圾邮件法案》来实施。[1846] 该法案旨在创建一个单独的国家标准，以便控制商务电子邮件。[1847] 它适用于商务电子消息，但不适用于那些与业务以及现有商业关系有关的消息。管制方法要求商务电子消息包括指明请求发送，包括自愿退出指令和发送者物理地址。[1848] 18 U.S.C. § 1037 对垃圾电子邮件的发送者定罪，尤其当他们篡改电子邮件的报头信息以绕过过滤技术时。[1849] 此外，该条款还对未获授权访问受保护计算机系统并启动多份商务电子邮件消息发送的行为予以定罪。

6.2.15 设备滥用

另一个严重的问题是设计用来实施犯罪的软件和硬件工具的可用性。[1850] 除了“黑客设备”的大量扩散，使未获授权的用户能够访问计算机系统的密码交换也是一项严峻的挑战。[1851] 这些设备的可用性及其潜在的威胁，使难以仅仅关注于对使用这些工具来实施犯罪的行为进行定罪。除了“违法行为的企图”之外，大多数国家刑法体系有一些针对准备和制造这些工具的行为进行定罪的条款。与此类设备传播行为作斗争的一种方法是，对工具的制造予以定罪。一般地，这种定罪 — 通常伴随广泛的刑事责任前移 — 限于最严重的罪行。特别是在欧盟的法律中，存在向不太严重违法行为定罪的准备活动延伸的趋势。[1852]

《网络犯罪公约》

考虑到欧洲理事会的其他举措，《网络犯罪公约》的起草者将以下特定的违法行为认定为独立的犯罪行为，即出于破坏计算机系统或数据的机密性、完整性和可用性的目的，滥用某些设备或访问数据。[1853]

条款

第 6 条— 设备滥用

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

(a) 制作、销售、为使用而取得、输入、发行或以其他方式使之可用于：

(i) 被设计或改装成主要用于上述 2-5 条所确定的任何违法行为的设备，包括计算机程序；

(ii) 可以进入整个或任何部分计算机系统的计算机密码、访问密码或类似数据，用以实施第 2-5 条中所确定的任何违法行为；以及

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

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

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

所涉及的对象

第 1(a)段确定了设计用于实施和推动网络犯罪的设备，[1854] 以及能够实现对计算机系统访问的密码。“设备”这一术语涵盖用于实施上述违法行为之一的、基于硬件和软件的解决方案。例如，《解释性报告》中提到的软件，诸如病毒程序或者为实现对计算机系统的访问而设计或改编的程序。[1855]“计算机密码、访问密码或类似的数据”不同于设备，它们不执行操作而是访问密码。在这一情况下中讨论的一个问题是，公布系统弱点是否属于本条款的范畴。[1856] 与典型的访问密码系统不同，系统漏洞并不一定使别人能够迅速访问计算机系统，而是使违法者能够利用弱点来成功攻击计算机系统。

涉及的违法行为

《网络犯罪公约》对众多违法行为予以定罪。除了对制作进行定罪之外，它还对销售、为使用而购买、进口、分发或以其他方式使装置和密码可用的行为进行制裁。在欧洲关于协调版权[1857] 的法律中可以找到一种类似的方法（限于设计用来绕过技术措施的装置），同时，许多国家已经在其刑法中执行了类似条款。[1858]“分发”指的是主动向他人提供转发设备或密码的行为。[1859] 参照第 6 条的规定，“销售”指的是为获得金钱回报或其他报酬而销售设备和密码的行为。“为使用而购买”涉及主动获取密码和装置有关的行为。[1860]“购买”行为与此类工具的使用相关，这一事实一般要求违法者具有以下意图，即在取得这些工具后，将其用于“实施第 2-5 条所规定之违法行为”，这超出了“正常的”意图。“进口”指的是从外国获得设备或访问口令的行为。[1861] 因此，为销售而进口这类工具的违法者可以在其销售这些工具之前被起诉。考虑到只有因使用而购买这类工具才会被定罪，这样就出现一个问题，那就是不带有任何销售和使用目的的进口行为是否属于《欧洲网络犯罪故意》第 6 条所涵盖的范畴。“使可用”指的是使其他使用者能够使用上述工具或代码。[1862]《解释性报告》建议，术语“使可用”还涉及到创建或编辑超级链接，以便使其他人能够使用这类设备。[1863]

双重使用工具

与欧盟协调版权的[1864]的方法不同，该条款不仅适用于那些专门设计用来为实施网络犯罪提供方便的工具—《网络犯罪公约》还涵盖那些通常用于合法目的的工具，而违法者的特定意图是实施网络犯罪。在《解释性报告》中起草者建议，将定义限定在专门设计用来实施网络犯罪的工具上有些不够宽泛，可能导致在证明犯罪诉讼中出现难以克服的困难，使该条款事实上无法适用或者只能对少数情形适用。[1865]

为确保实现对计算机系统的适当保护，专家们使用和拥有各种各样的软件工具，使自己能够集中于执法。《网络犯罪公约》以三种方式解决这些利害关系：[1866]它使第 6 条 1（b）段中的各方能在以下方面作一些保留，即在确定刑事责任之前规定可以拥有此类物品的最小数量。除了这一点，对拥有这些装置的行为定罪，限于要求拥有者具备利用此类工具实施《网络犯罪公约》第 2-5 条中所规定的违法行为的意图。[1867]《解释性报告》指出，将这种特殊的意图纳入，是为了“避免对出于合法目的而制造和销售此类工具的行为出现过度定罪的危险，比如，为了对付针对计算机系统的攻击等。”[1868]最后，《网络犯罪公约》的起草者在第 2 段中明确声明，该条款不包括为授权测试或为保护计算机系统而制造此类工具的行为，其原因是该条款专指未获授权行为。

对拥有进行定罪

第 1(b)段进一步强化了第 1(a)段中的规定，方法是，如果拥有装备或密码的行为与实施网络犯罪的意图有关，那么予以定罪。对拥有此类工具进行定罪是有争议的。[1869]第 6 条不限于专门设计用于实施犯罪的工具，而对其定罪的反对者担心，对拥有此类工具的行为进行定罪，可能对系统管理员和网络安全专家构成不可接受的风险。[1870]《网络犯罪公约》使各方能够在附带刑事责任之前要求拥有一定数量的此类工具。

主观因素

与欧洲理事会《网络犯罪公约》定义的所有违法行为一样，第 6 条要求违法者是故意实施违法行为。[1871]除了所涉及行为的普通意图之外，《网络犯罪公约》第 6 条还要求具备其他特殊意图，即将工具用于实施《网络犯罪公约》第 2-5 条中所确定的任何一种违法行为。[1872]

未获授权

与上面讨论的条款类似，这些行为必须是“未获授权”而实施的。[1873]至于担心该条款可能被用来对自我保护措施中的软件工具的合法操作行为进行定罪，《网络犯罪公约》的起草者指出，此类行为不会被视为“未获授权”。[1874]

限制与保留

由于是否需要对拥有这种工具的行为进行定罪还存在争议，因此《网络犯罪公约》在第 6 条第 3 段（除了第 1(b)段第 2 句）给出了复杂的保留选择方案。如果签约方使用这种保留权利，那么它可以不对拥有这类工具的行为以及大量依据第 1 段的(a)分段认为有罪的违法行为定罪——例如，制造此类工具。[1875]

英联邦计算机及计算机相关犯罪示范法

在 2002 年的《英联邦示范法》第 9 节中可以找到一种与《网络犯罪公约》第 6 条相一致的方法。[1876]

非法设备

9.

(1) 如果某人：

(a) 没有合法或正当的理由，有意或不计后果地制作、销售、为使用而取得、进口、出口、发行或以其他方式利用：

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

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

意图使任何人都可以用来实施如第 5、6、7 或 8 节所述的违法行为；或者

(b) 拥有一件第 i、ii 小段中提及的工具，意图使任何人都可以用来实施如第 5、6、7 或 8 节所述的违法行为。

则被认定为犯罪

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

虽然与本条款所涉及的工具和行为相同，但《英联邦示范法》与《网络犯罪公约》的主要区别在对不计后果的行为进行定罪。在《英联邦示范法》进行谈判的过程中，就对拥有此类工具的行为进行定罪的条款的进一步修正意见进行了讨论。专家组建议，对拥有多个此类工具的违法者进行定罪。[1877] 加拿大提出了一种不预先确定工具数量而进行定罪的类似方法。[1878]

《斯坦福国际公约》草案

1999 年的非正式 [1879] 《斯坦福国际公约》草案（简称“斯坦福草案”）包含一条对使用非法工具进行定罪的条款。

第 3 条— 违法行为

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

[...]

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

《公约》起草者指出，通常情况下，根据《斯坦福公约》草案，没有哪种类型的言论或出版物要求被视为犯罪行为。[1880] 唯一例外就是与非法设备有关的言论和出版物。[1881] 起草者强调，在这种情况下，定罪应仅限于提到的行为，比如，在对系统弱点进行讨论时未涵盖的行为。[1882]

《HIPCAR 网络犯罪立法文本》

在立法文本中有一种 HIPCAR 创立之初由受益国提出的有趣的方法。[1883]

> **非法设备**
> 10.
> *[...]*
> (3) 如果某个国家有有效的补救措施，可以决定不对单纯的无授权访问定罪。此外，各国可以决定限制针对所列设备的定罪范围。

为防止定罪范围过宽，起草者决定通过引入黑名单的形式来增加限制定罪的可能性。在这种情况下，只有黑名单的设备才被列入条款。从网络安全的角度看，这样的方法可以限制定罪过宽的风险。然而，维护这样一份黑名单非常有可能需要有有意义的资源。

6.2.16 与计算机有关的伪造

涉及与计算机有关的伪造的刑事诉讼案件过去很少见，原因是大多数法律文件都是有形文件。随着数字化的发展，这种情形正在发生变化。[1884] 数字化文件的趋势得到了为其使用所建立的法律背景的支持，例如，数字签名的法律鉴别。此外，针对与计算机有关的伪造的条款，在对抗“网络钓鱼”的过程中发挥着重要作用。[1885]

欧洲理事会《网络犯罪公约》

大多数刑法体系都对伪造有形文件予以定罪。[1886] 《网络犯罪公约》的起草者指出，教条式的国家立法结构正在改变。[1887] 一种概念是基于文件作者的真实性，而另一种概念是基于声明的真实性。起草者决定执行最低标准，通过认定类似于伪造传统有形文件的违法行为的方式保护电子数据的安全性和可靠性，以填补刑法可能不适用于以电子方式存储的数据的空白。[1888]

条款

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

所涉及的对象

与计算机有关的伪造，其目标是数据——不管它们是否可直接可读和/或可理解。《网络犯罪公约》[1889] 将计算机数据定义为“事实、信息或概念的某种表述，它以一种适于在计算机系统中进行处理的形式存在，包括适于促使计算机系统执行某种功能的程序”。该条款不仅仅指作为上述其中一种行为目标的计算机数据。此外，还有必要包括导致不真实数据的各种行为。

第 7 条要求（至少在主观因素方面）数据相当于公共或私人的文件。这意味着数据必须是法律上相关的[1890]：对伪造不能合法使用的数据的行为，没有包括在这一条款中。

涉及的违法行为

数据“输入”[1891]必须与制作一份虚假的有形文件相对应。[1892]“更改”这一术语指的是对现有数据进行修改。[1893]《解释性报告》中专门指出了各种不同的更改和部分更改。[1894]计算机数据的“限制”这一术语指的是影响数据可用性的行为。[1895]在《解释性报告》中，起草者专门提到了隐瞒或隐藏数据的行为。[1896]比如，这一行为可以通过在自动创建电子文件期间阻止某些来自数据库的信息来实施。“删除”这一术语对应第 4 条中的该术语的定义，涉及移除信息的各种行为。[1897]《解释性报告》只提到了从数据介质中移除数据。[1898]但条款的适用范围强烈支持拓宽“删除”这一术语的定义。基于这种更加广义的定义，“删除”行为既可以通过移除整个文件来实施，也可以通过部分删去文件中的信息来实施。[1899]

主观因素

与欧洲理事会《网络犯罪公约》所定义的所有其他违法行为一样，第 3 条要求违法者故意实施了违法行为。[1900]《网络犯罪公约》没有包含对“故意”这一术语的定义。在《解释性报告》中起草者指出，“故意”这一用语应在国家层面上进行定义。[1901]

未获授权

只有当伪造行为是“未获授权”时实施的，才可根据《公约》第 7 条予以起诉。[1902]

限制与保留

第 7 条还提供了作出保留以便限制定罪的可能性，方法是要求在界定刑事责任之前需具备其他因素，如诈骗意图。[1903]

《英联邦计算机及计算机相关犯罪示范法》

2002 年的《英联邦示范法》没有包含任何对与计算机有关的伪造进行定罪的条款。[1904]

《斯坦福国际公约》草案

1999 年的非正式[1905]《斯坦福国际国公约》草案包含一条对伪造计算机数据的行为进行定罪的条款。

> **第 3 条— 违法行为**
> 1. 根据本《公约》，如果任何人在未获得法律认可的授权、许可或同意的情况下非法且故意从事以下任何行为，即认为是在实施违法行为：
> [...]
> (b) 出于供错误信息，以便对个人或财产造成实质性损坏以及为了产生相应的不良效应的目的创建、存储、更改、删除、传输、转移、误传、操纵或干扰网络系统中的数据或程序；
> [...]

与《网络犯罪公约》第 7 条的主要区别在于：第 3 条 1b) 款并不局限于单纯的操纵数据，而是要求对计算机系统的干扰。欧洲理事会《网络犯罪公约》第 7 条不要求此类行为，而只要违法者的意图是希望被人认为是合法的或者其行为看起来像是出于合法的目的就足够了。

6.2.17 身份盗用

考虑到媒体的覆盖范围，[1906] 该领域的最新调查结果 [1907] 以及大量的法律和技术出版物[1908] 将身份盗用描述成一种普遍现象看起来并不为过。[1909] 尽管这种现象存在于世界各地，但并非所有国家都已在其国家刑法体系中执行了对所有涉及身份盗用的行为进行定罪的条款。欧盟委员会最近声明，对身份盗用，尚未在所有欧盟成员国中都予以定罪。[1910] 该委员会表明了自己的立场，即“如果所有成员国都对身份盗用进行定罪，那么欧盟的执法合作将更加紧密”，委员会还宣布，它将立即着手进行磋商，以评估该法律是否恰当。[1911]

在与身份盗用作斗争的过程中，相比现有的法律手段，存在许多问题，其中之一是它们存在巨大差异。[1912] 现有方法之间唯一一致的因素是，被判有罪的行为与下列各阶段中的一个或多个阶段有关：[1913]

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

根据这种观察，对身份盗用进行定罪一般有两种系统的方法：

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

单一条款方法实例

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

第 1028 段. 与身份识别文件、身份验证特征和信息有关的欺诈行为及相关活动

(a) 无论何人，在本节中(c)小节所述的情形下：

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

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

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

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

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

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

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

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

将处以本节第（b）小节中所述的处罚。

[…]

第 1028A 段. 严重的身份盗用行为

(a) 违法行为 —

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

[…]

第 1 阶段

为了实施与身份盗用有关的犯罪活动，违法者需要拥有与身份相关的数据。[1914] 通过对本着犯罪意图而“传输”身份识别方法的行为进行定罪，这些条款以非常广泛的方式对与第 1 阶段有关的行为进行定罪。[1915] 由于这些条款着重于传输行为，因此它们没有涵盖由违法者在开始传输过程之前实施的违法行为。[1916] 其他一些可以用来从受害者处获取与计算机身份有关的数据的违法行为，如发送网络钓鱼邮件和设计恶意软件等，没有包括在 18 U.S.C. § 1028(a) (7)和 18 U.S.C. 1028A(a) (1)中。

第 2 阶段

通过对本着实施犯罪的意图而拥有的行为进行定罪，条款再次采用了一种广泛的方法来对与第 2 阶段有关的行为进行定罪。尤其包括以下违法行为，即拥有与身份有关的信息的目的是为了之后用它们来实施一种与身份盗用有关的、典型的违法行为。[1917] 拥有与身份有关的数据而无意使用它们，则不在条款的覆盖范围内。[1918]

第 3 阶段

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

另一实例是 HIPCAR 创立之初制定的《网络犯罪立法文本》第 14 节中给出的条款。[1919]

身份盗用相关犯罪

14.

任何人，如果故意在没有合法的借口或理由或超出合法借口或理由的范围的情况下，在违法行为的各个阶段利用计算机系统故意在没有合法借口或理由的前提下传送、拥有或使用其他人的身份信息，目的在于实施、协助或支持或介入任何构成犯罪的非法活动，则判定其实施了该处罚的犯罪行为，定罪时，可处以不超过[具体期限]的监禁，或不超过[一定数额]的罚金，或二者并罚。

该条款涵盖了上述典型身份犯罪的各个阶段。只有第 1 阶段（在这个阶段违法者获取了与身份有关的信息）没有涵盖其中。“传送”身份信息涉及从一个计算机系统到另一计算机系统传送数据的过程。这一行为尤其指出售（和相关转让）与身份有关的信息。[1920] “拥有”指的是一个人故意实施的控制与身份有关的信息的行为。“使用”涉及范围更广的行为，例如将身份信息放在网上出售。在主观因素方面，该条款要求违法者故意在所有客观因素下另外还有实施、协助或只支持任何超出传送、拥有后使用身份信息范围的非法行为的主观故意。

多种条款方法实例

欧洲理事会《网络犯罪公约》与单一条款方法（如美国方法）之间的主要区别在于《网络犯罪公约》没有定义一种非法使用身份相关信息的单独的网络违法行为。[1921] 类似于对获取身份相关信息的违法行为进行定罪的情形，《网络犯罪公约》没有涵盖与非法使用个人信息有关的、所有可能的行为。

第 1 阶段

针对第 1 阶段，欧洲理事会《网络犯罪公约》[1922] 包含许多对与互联网有关的身份盗用行为进行定罪的条款。特别是以下三条：

- 非法访问（第 2 条）；[1923]
- 非法监听（第 3 条）；[1924]
- 数据干扰（第 4 条）；[1925]

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

第 2 阶段

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

第 3 阶段

《欧洲网络犯罪的公约》定义了大量与网络犯罪有关的违法行为。其中的一些违法行为是作案者使用与身份有关的信息来实施的。一个例子是与计算机有关的欺诈，它常常在身份盗用的背景下被提及。[1926] 关于身份盗用的调查指出，大多数以非法手段获取的数据都被用来实施信用卡欺诈。[1927] 如果信用卡欺诈是在线实施的，那么有可能根据《网络犯罪公约》第 8 条来起诉作案者。其他

可通过使用身份相关信息来实施的违法活动，如果这些信息是过去获取的、且未在《网络犯罪公约》中提及，那么不在该法律框架的覆盖范围内。如果违法者本着隐藏其身份的目的而使用与身份有关的信息，那么要起诉他尤其是不可能的。

6.2.18 与计算机有关的欺诈

故意欺诈是网络空间里一种普遍存在的犯罪。[1928] 在互联网之外，它也是一种普遍问题，因此，大多数国家法律包含对此类违法行为进行定罪的条款。[1929] 不过，将现有条款用于与互联网有关的案件存在一些困难，原因是传统的国家刑法条款是基于个人的欺诈。[1930] 事实上，在许多借助互联网实施的欺骗案件中，正是计算机系统对违法者的行为进行响应。如果传统的打击欺诈的刑法条款没有涵盖计算机系统，那么有必要对国家法律进行更新。[1931]

欧洲理事会《网络犯罪公约》

通过提供一条针对与计算机有关的欺诈的条款，《网络犯罪公约》力图对任何不恰当操纵数据处理过程，意在影响财产的非法转移的行为予以定罪：[1932]

条款

第 8 条—计算机有关的欺诈

当以下对他人财产是进行时，各方应采取必要的法律措施和其他措施，依据本国法律将未经授权而故意实施且造成了损失的违法行为判定为犯罪行为。

a. 任何输入、更改、删除或限制计算机数据的行为；

b. 任何干扰计算机系统正常运转的行为，这些行为本着欺骗性的或不诚实的意图，在未经授权的情况下为自己或他人获取经济利益。

涉及的违法行为

第 8 条 a)包含了一个与计算机有关的欺诈行为最为相关的违法行为清单。[1933]“输入”计算机数据包括所有类型的输入操纵，比如向计算机输入不正确的数据、操纵计算机软件以及其他干扰数据处理过程的行为。[1934]“更改”这一术语指的是修改现有数据。[1935]“限制”计算机数据这一术语指的是影响数据可用性的行为。[1936]“删除”这一术语对应第 4 条中的术语定义，涵盖移去信息的各种行为。[1937]

除了列举违法行为之外，第 8 条 b）分款包含一条普通条款，该条款对与欺骗有关的“干扰计算机系统的正常运转”行为予以定罪。该普通条款添加到了所涉及行为的列表中，以便给条款的进一步完善留下空间。[1938]

《解释性报告》指出，“干扰计算机系统的正常运转”涵盖操纵硬件、限制打印资料、影响数据记录与流动或影响程序运行次序等行为。[1939]

经济损失

依据大多数国家刑法，犯罪行为必须造成经济损失。《网络犯罪公约》采用了一种类似的概念，仅对那些对他人的财产造成了直接的经济损失或所有权损失，包括金钱损失、有形和无形的经济价值损失等的操纵行为予以定罪。[1940]

主观因素

与其他列举的违法行为一样，欧洲理事会《网络犯罪公约》第 8 条要求违法者故意实施违法行为。这种意图指的是故意操纵以及故意造成经济损失。

此外，《网络犯罪公约》要求违法者的行为具有欺骗或不诚实意图，以便为自己或他人牟取经济利益或其他利益。[1941] 作为由于缺少特殊意图而不承担刑事责任行为的例子，《解释性报告》提到了源自市场竞争的商业作法，这些作法可能给某人造成经济损失但给另一人带来经济利益，但它们的实施不具备欺骗或不诚实意图。[1942]

未获授权

只有当访问是“未获授权”时，才能根据《网络犯罪公约》第 8 条对与计算机有关的欺骗行为进行起诉。[1943] 这包括要求所获得的经济利益是未获授权的。《网络犯罪公约》的起草者指出，根据相关各方签订的有效合同而实施的行为，不被视为未获授权。[1944]

《英联邦计算机及计算机相关犯罪示范法》

2002 年的英联邦示范法没有包含针对计算机欺诈的定罪的条款。[1945]

《斯坦福国际公约》草案

1999 年的非正式[1946] 《斯坦福国际公约》草案没有包含针对计算机欺诈定罪的条款。

6.2.19 版权犯罪

在发行版权保护内容过程中模拟到数字的转换，标志着在版权侵权中出现了转折点。[1947] 对音乐和视频作品的复制，过去一直限于对模拟资源的复制，常常会造成复制品质量的下降，这反过来限制了使用复制品进行下一步复制的选择。随着向数字资源的转换，复制的质量得以保证，保持复制品质量的一致已成为可能。[1948]

通过实施一些技术手段（数字版本管理或 DRM）来防止复制，娱乐行业已经对复制问题作出了响应，[1949] 但迄今为止，在被引入后不久，这些技术手段往往被违法者绕过。[1950] 互联网上涌现出各种各样可用的软件工具，使用户能够拷贝受 DRM 系统保护的音乐 CD 和电影 DVD。此外，互联网提供了不受限分发的机会。结果是，侵犯知识产权（尤其是版权）的行为是通过互联网广泛实施的一种违法行为。[1951]

欧洲理事会《网络犯罪公约》

《网络犯罪公约》包含一条涉及上述版权犯罪行为的条款，力图协调各国法律中的诸多不同。结果是，这一条款却成为《网络犯罪公约》在欧洲以外的国家应用的主要障碍之一。

第 10 条— 破坏版权或相关权利的违法行为

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

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

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

在有些国家[1952]，侵犯版权是犯罪行为，这种行为在很多国际条约中得以体现。[1953]《网络犯罪公约》旨在为侵犯版权的定罪问题提供基本原则，以便协调现有法律之间的不同。这一条款没有涵盖专利或商标侵权行为。[1954]

参考的国际协定

与其他法律框架不同，《网络犯罪公约》并没有明确指定哪些行为将被定罪，而是参照了大量的国际协定。[1955] 这也是第 10 条备受批评的一个方面。这使得更难发现定罪的程度，而且这些协定可能在随后出现变更，除此之外，如果《网络犯罪公约》责成各签字国签署第 10 条中提到的国际协定，那么问题就出现了。《网络犯罪公约》的起草者指出，欧洲理事会《网络犯罪公约》不得引入任何此类义务。[1956] 这样，那些尚未签署上述国际协定的国家，既不一定要签署协定，也不会被迫对与它们尚未签署的协定有关的犯罪行为进行定罪。因此，第 10 条仅仅对那些已经签署了上述协定的国家具有约束力。

主观因素

由于其一般性，《网络犯罪公约》将定罪限定于那些借助计算机系统实施的违法行为。[1957] 除了通过计算机系统实施的犯罪行为之外，刑事责任也限定于那些故意实施的违法行为和大规模的违法行为。“故意”这一术语与《网络犯罪公约》其他实体法律条款中使用的“故意”这一术语是对应的，并且考虑到了《TRIPS 协定》第 61 条中[1958] 使用的术语，该协定用于监管对版权侵犯行为进行定罪的义务。[1959]

商业规模

对违法行为须是大规模实施的这一限定，也考虑到了《与贸易有关的知识产权协定》（TRIPS），该协定要求刑事制裁只针对“商业规模的盗版行为”。由于文件共享系统中的大多数版权侵权行为并不是大规模实施的，因此，它们未被第 10 条所涵盖。《网络犯罪公约》力图为有关互联网的违法行为制定一些最低标准。因此，各方可以在对版权侵权犯罪定罪的过程中超越“商业规模”这一界限。[1960]

未获授权

一般地，由欧洲理事会《网络犯罪公约》定义的实体刑法条款要求违法行为是“未获授权”而实施的。[1961]《网络犯罪公约》的起草者指出，“侵犯”这一术语已经暗示了该行为的实施是未获授权的。[1962]

限制与保留

第 3 段的条款可以使各签约国做出保留，只要有其他有效的补救措施可用，且所作保留无损各签约国的国际义务。

《斯坦福国际公约》草案

1999 年非正式的[1963]《斯坦福国际公约》草案（简称“斯坦福草案”）没有包括对侵犯版权行为定罪的条款。《斯坦福草案》起草者指出，版权犯罪之所以没有包含在内，是因为这可能已被证明困难的。[1964] 相反，他们直接参考了现有的国际协定。[1965]

6.2.20 网络恐怖主义

如上所述，术语“网络恐怖主义”用于描述一系列从宣传到针对攻击目标的活动。在法律对策方面，有可能分为三种不同的系统方法。

系统方法

使用现有的网络犯罪立法

第一种方法是使用现有的网络犯罪立法（为涵盖非恐怖主义行为而制定）来对网络恐怖主义进行定罪。在这种背景下，需要考虑三个方面的情况。一是涵盖非恐怖主义行为的实体刑法条款，如系统干扰[1966]可能适用于恐怖主义行为，但通常的量刑范围可能会与专门的恐怖主义立法不同。这可能会影响到局限于恐怖主义的复杂调查工具的使用能力和或组织犯罪调查能力。二是在网络恐怖主义面临较少的困难的情况下，针对网络犯罪调查工具的使用，以至于大多数国家对一般的网络犯罪（包括任何涉及计算机数据的违法行为）不限制使用复杂的调查工具。三是用于解决网络犯罪问题的地区性法律文本（并非专用），网络恐怖主义通常包含免除与政治犯罪有关的国际合作的行为。欧洲理事会《网络犯罪公约》第 27 条 4a)款给出了一个具体实例。[1967]

第 27 条—在没有适用国际协议的情况下提出相互协助请求的程序

[…]

4. 除第 25 条第 4 款所规定的拒绝条件之外，如果有下列情形，被申请求方可以拒绝协助：

a 请求涉及违法行为，被请求方认为是政治犯罪或与政治犯罪有关的违法行为；

b 被请求方认为，对请求的执行有可能损害主权、安全、公共秩序或其他本质利益。

[…]

该条款授权各签约国，如果他们认为是政治犯罪或与政治犯罪有关的违法行为，可以拒绝互相援助。这有可能给调查工作带来严重的障碍。因此，针对恐怖主义的法律框架，如 2005 年的《欧洲理事会防止恐怖主义公约》[1968] 包含一条排除政治例外的条款。

第 20 条— 排除政治例外的条款

1 如果出于引渡或双方合法援助的目的，则本公约第 5-7 条中所列的犯罪行为都不应看作政治犯罪、与政治犯罪有关的犯罪或受政治动机鼓动的犯罪行为。因此，基于上述情况的引渡或双边合法援助请求不能因认为是政治犯罪、与政治犯罪有关的犯罪或受政治动机鼓动的犯罪行为被拒绝。

[…]

使用现有的反恐怖主义立法

第二种方法是使用现有针对恐怖主义的立法来对起诉和定罪网络恐怖主义。这类传统条款的具体事例有 2005 年的《欧洲理事会防止恐怖主义公约》。[1969]

第 5 条— 公开挑衅实施恐怖主义犯罪

1. 出于本公约的目的，公开挑衅实施恐怖主义犯罪指的是带有鼓动实施恐怖主义犯罪的目的，向公众散播或提供消息的行为，该行为有可能导致一起或多起危险犯罪行为的危险后果。

2. 各方应采取必要的措施，依据本国法律将不合法故意实施的第 1 段所定义的公开挑衅实施恐怖主义活动认定为犯罪行为。

第 6 条— 为恐怖主义招募人员

1. 出于本公约的目的，为恐怖主义招募人员指的是招揽其他人实施或参与恐怖主义犯罪，或使这些人加入协会或组织，目的是通过这些协会和组织实施犯罪行为

2. 各方应采取必要的措施，依据本国法律将不合法故意实施的第 1 段所定义的为恐怖主义招募人员的行为认定为犯罪行为。

《防止恐怖主义公约》包含若干种犯罪行为，如，公开宣传恐怖注意犯罪和为恐怖主义招募人员，但不包含针对计算机系统实施恐怖主义攻击的定罪条款。此外，公约还不包含诉讼条款。尤其是对网络犯罪的调查，通常需要专门的诉讼条款。确认一名违法者利用网站宣传恐怖主义要求复杂的法律条款，例如流量数据的快速留存。

专门立法

第三种方法是制定专门的立法来解决网络恐怖主义问题。

专门立法的实例

如上所述，术语“网络恐怖主义”用于描述一系列从宣传到定点攻击的活动。在法律对策方面有两个主要方面的规定——有关计算机的攻击和非法内容。

与计算机有关的攻击

一种专门解决恐怖主义计算机攻击的方法是 2008 年修订的《印度信息技术法案 2000》第 66F 节中的条款：

***66F* 针对网络恐怖主义的处罚——信息技术法案 2000**。[修订版为信息技术法案（修正案）2008]。

(1) 无论何人——

(A) 通过下列手段，故意威胁印度的统一、完整、安全或主权，或故意在人民或任何一部分人民中间引起恐慌——

(i) 使任何有权访问计算机资源的人无法访问或导致其无法访问计算机资源；或

(ii) 在未获授权或超出访问权限的情况下，试图进入或访问计算机资源；或

(iii)使用或导致使用恶意软件。

并且这类行为将要或有可能造成人员伤亡或财产损失或破坏或引起恐慌，或明知有可能引起社会生活必需物资供应或服务的损失或破坏，或者负面影响第 70 节规定的关键信息基础设施；或

(B) 在未获授权或超出访问权限的情况下，故意进入或访问某一计算机资源，并且通过这种行为能够获取信息、数据或访问计算机数据库，并且相信这类信息、数据或计算机数据库可以用于损害或有可能损害印度主权和完整的利益、国家安全、与外国的友好关系、公共秩序、道德或礼仪，或造成藐视法庭、中伤或煽动犯罪，或损害外来民族、团体或其他人的利益，则认定其犯有网络恐怖主义罪。

(2) 任何实施或共谋实施网络恐怖主义犯罪的人应处以最高至终生监禁的处罚。

《印度信息技术法案》第 66F 节不仅要求违法者抱有恐怖主义意图来实施犯罪（“故意威胁印度的统一、完整、安全或主权，或故意在人民或任何一部分人民中间引起恐慌”），而且还要求犯罪行为造成严重的损失，如人员伤亡或破坏关键信息基础设施服务）。

非法内容

诸如恐怖主义宣传之类的非法内容是各国明确坚持采用技术中立非法的一个领域。2006 年 7 月 27 日颁布的《俄罗斯联邦关于信息、信息技术和信息保护法 149-FZ》第 10 条就是这类技术中立非法的一个具体实例。

第 10 条— 传播信息或提供信息

[…]

6. 禁止传播有关战争宣传、民族、种族或宗教歧视和敌视的信息以及其他信息，传播这类信息要受到法律制裁或承担行政责任。

这一条款没有专门针对利用计算机网络传播非法内容或使这些非法内容在网络中可以被访问的问题，而是以技术中立的方法制定该条款。

2008 年的《欧盟理事会反对恐怖主义框架决议修正案》[1970]第 3 条是这类技术中立方法的另一实例。[1971]

第 3 条— 与恐怖主义有关的犯罪行为

1. 出于本框架决议的目的：

(a) “公开宣传实施恐怖犯罪”系指向公众传播或提供信息，旨在鼓动实施第 1 条(1)款(a)-(h)项所列犯罪行为之一，不论是否宣传恐怖犯罪，这类行为都有可能导致实施一起或多起犯罪活动；

(b) “为恐怖主义招募人员”系指招募其他人实施第 1 节(1)款(a)-(h)项或第 2 节(2)款中所列的犯罪行为之一；

(c) “为恐怖主义作培训”系指明知其所传授的技能能够用于实施第 1 节(1)款(a)- (h)项所列的犯罪行为的目的而为制作或使用炸药、枪炮或其他武器或有毒有害物质作指导，或为专门的方法或技术作指导。

2. 各国应采取必要的措施确保与恐怖活动有关的犯罪包括下列故意行为：：

(a) 公开宣传实施恐怖犯罪；

(b) 为恐怖主义招募人员；

(c) 为恐怖主义作培训；
(d) 出于实施第 1 条(1)款所列的犯罪行为而实施严重盗窃；
(e) 出于准备第 1 条(1)款所列的犯罪行为而进行勒索；
(f) 出于实施第 1 条(1)款(a)-(h)项和第 2 条(2)款(b)项所列的犯罪行为而拟定错误的行政文件。
3. 对于第 2 段中所列的犯罪行为，恐怖犯罪不需要真正实施。

起草者在介绍中强调，现有法律框架只对协助、支持和鼓动恐怖主义犯罪定罪，而不对通过互联网宣传专门的恐怖知识进行定罪。在这种情况下，起草者指出："互联网用于在欧洲鼓动和动员地区性恐怖组织网和恐怖分子，并且用作传播恐怖手段和恐怖方法的源头，因而其作用属于一个'虚拟训练营'。"[1972] 尽管在介绍中很明确地提到了网络恐怖主义，但制定该条款仍采用技术中立的方法，将网上和网下的恐怖主义训练列入其中。[1973] 在于互联网有关的案件中应用这一条款的一个问题是难于证明违法者的行为是在明知其所提供的技能有可能用于犯罪的目的的情况下实施的。对这类证据的需求很有可能限制该条款在针对网上武器使用指导方面的适用性。由于武器和爆炸物可以用来实施常规犯罪和恐怖犯罪，所以，单纯公开这类信息不能证明信息发布者知道如何使用这些信息。因此，需要考虑信息发布的背景（例如，公布信息的网站是由恐怖组织所控制）。如果所发布的信息超出其他恐怖内容的范围（如，通过文件共享系统或文件托管服务），就会出现问题。

《计算机信息网络互联网安全保护管理办法》第 5 条是了专门针对互联网的方法的一个实例：

第 5 条: 任何单位和个人不得利用国际联网制作、复制、查阅和传播下列信息：

(1) 煽动抗拒、破坏宪法和法律、行政法规实施的；
(2) 煽动颠覆国家政权，推翻社会主义制度的；
(3) 煽动分裂国家、破坏国家统一的；
(4) 煽动民族仇恨、民族歧视，破坏民族团结的；
(5) 捏造或者歪曲事实，散布谣言，扰乱社会秩序的；
(6) 宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；
(7) 公然侮辱他人或者捏造事实诽谤他人的；
(8) 损害国家机关信誉的；
(9) 其他违反宪法和法律、行政法规的。

网络战争

虽然与网络战争有关的威胁已经讨论了几十年，但有关法律对策的争论才刚刚开始。网络战争高于网络犯罪，它受国际法的管制。《海牙公约》、《日内瓦公约》和联合国宪章是国际法中的重要法律文本，其中包含战争法的条款。虽然应用这些条款来调节武装冲突具有很好的先例，但将其应用于网络和基于网络的攻击时，就会遇到困难。这一点可以通过分析《联合国宪章》第 2 条第（4）款——禁止使用武力来说明。

联合国宪章第 2 条

为求实现第 1 条所述各宗旨起见，本组织及其会员国应遵行下列原则。

[...]

(4) 各会员国在其国际关系上不得使用威胁或武力，或以与联合国宗旨不符之任何其他方法，侵害任何会员国或国家之领土完整或政治独立。

[...]

禁止使用武力的目的是全面禁止使用各种武力，符合《联合国宪章》的武力除外。[1974] 最近几十年，第 2 条第（4）款中禁止使用武力的要求已受到数次挑战。其中的主要挑战之一已经从大规模战争（这是二战后起草的《联合国宪章》的重点）转向如今时有发生的小规模战争。[1975] 计算机攻击又是一个新的挑战，不仅冲突的规模不同，而且冲突中使用的方法和工具上也不同。[1976] 因此，应用第 2 条面临的主要困难就是对“使用武力”这一术语的解释。《联合国宪章》以及相关国际法律都没有清楚地定义“使用武力”这一术语。《联合国宪章》并非禁止所有类型的敌对行动，这一事实已被广泛接受。例如，宪章涉及使用传统武器的攻击，但没有涉及武力威胁和经济压制。[1977]

使用武力的两个组成要素一是使用武器，二是使用武力的国家。虽然后者的重要性已经在 9·11 袭击后受到安理会决议的质疑，但这两个要素在禁止使用武力方面仍是必要的。

使用武器/破坏生命财产

第一个构成要素是使用武器。用于实施互联网攻击的计算机技术很难称得上是传统武器，因此，这类武器通常涉及动能冲击。[1978]不过，将化学武器和生物武器涵盖其中的需求已经要求人们的观念从基于行动的定义转向基于冲击的方法。在这样的广义方法下，武器可以被定义为摧毁生命或财产的工具。[1979]

但是，虽然以这类广义的解释为基础，将计算机和网络攻击看作使用武力，而将计算机看作武器仍是一个问题，因为攻击的冲击力发生了变化。[1980]与传统的武装冲突相比，不仅使用的方法发生了变化，而且其效果也有所不同。[1981]传统的涉及使用武力的军事战略重点在于物理上终结敌人的军事力量。计算机和网络攻击可以在最小的物理破坏和生命损失情况下来实施。[1982]不同于导弹攻击，能够暂时关闭政府网站的拒绝服务攻击并不能造成任何实际的物理伤害。但它却有可能使人误解为计算机攻击不能造成严重伤害。针对医院或血库计算机系统的拒绝服务攻击能够对健康造成严重的威胁，致大批民众的生命于危险之中。所发现的超级工厂病毒潜在的物理冲击是证明计算机攻击不一定没有非物理后果的另一实例。如果计算机和网络攻击具有这类物理冲击，可以认为这类攻击类似于传统武器。[1983]

国家间的冲突

如上所述，使用《联合国宪章》第 2 条的第二个要求是使用武力应该发生在两国之间。尽管目前正在拓宽《联合国宪章》的应用范围，但《联合国宪章》第 2 条中仍没有涵盖非国家行为体之间实施的行为。这与涵盖网络战争有很大的关系，因此，不同于传统战争，非国家行为体的作用更加重要。由于非国家行为体可以获得甚至有可能超出国家控制范围之外的强大资源，所以扩散问题饮起了人们的严重关切。[1984] 最大的僵尸网络拥有数百万计算机系统。在大多数国家，这一数字有可能大于国家控制的用于军事干预的计算机系统的数量。非国家行为体的能力是高度相关的，因为非国家行为体主要游离于约束国家的国际法律框架之外行动。这就增大了对归属问题的关注度。迄今为止，《联合国宪章》第 2 条的用于要求计算机攻击能够追溯到国家。2007 年爱沙尼亚和 2008 年格鲁吉亚事件的经验表明，在大多数情况下，识别或查证攻击源头可能是一个不可逾越的障碍。

6.3 数字证据

参考书目（节选）： *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf; *Gercke*, Impact of Cloud Computing on the work of law enforcement agencies, published in *Taeger/Wiebe*, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-mail: A Trusted E-mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4; *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No.3; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002; *Hayes*, Forensic Handwriting Examination, 2006; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2; *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010; *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No.1; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38;

Siegfried/Siedsma/Countryman/Hosmer, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1; *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

由于硬盘驱动器容量[1985]的增加，以及与存储物理文件相比，数字文件存储成本的下降[1986]，数字文件的数量与日俱增。[1987]如今，相当大数量的数据以数字形式存储。[1988]此外，计算机和网络技术已经成为发达国家日常生活的一部分，在发展中国家，其数量也在增加。因此，文本文件、数字视频数字图片[1989]等电子文件在网络犯罪调查和相关的法庭诉讼活动中发挥着重要的作用。[1990]

然而，数字化的冲击和数字证据的重要性正在拓宽网络犯罪调查的范围：即使是在实施常规犯罪时，犯罪分子也可能留下数字痕迹，例如，移动电话的位置信息[1991]或可疑的搜索引擎请求。[1992]因此，能够开发专用的数据调查工具并在法庭上呈送数字证据对于网络犯罪调查和常规犯罪调查都很有必要。[1993]

虽然处理"数字证据"面临很多挑战，[1994]但也为调查和鉴定专家和法院的工作提供了新的可能性。在第一阶段——收集证据阶段——处理数字证据的能力要求已经改变了调查员的工作。他们需要专门的调查工具来展开调查。如果没有指纹或目击证人这类传统证据，这类工具的实用性就显得尤为重要。在这种情况下，成功确认并起诉犯罪分子可以依据数字证据的正确收集和评价。[1995]然而，除收集证据之外，数字化还影响着执法机构和法院处理证据的方式。[1996]传统文件以向法院递交原件的形式出现，而在某些情况下，数字证据要求专门的程序，不能将数字证据转换为传统证据，例如，展示文件打印稿和其他发现的数据。[1997]

本节将介绍数字证据和网络犯罪调查的实际应用和法律方面的总体情况。

6.3.1 数字证据的定义

数字化和新兴的信息通信技术对收集证据以及在法庭上使用证据的诉讼过程产生了巨大的影响。[1998]作为发展的结果，数字证据已经被用作一种新的证据资源。[1999]电子或数字证据没有单独的定义。[2000]英国《警察与犯罪证据法》将数字证据定义为"计算机中包含的所有信息"。[2001]有一种广义的方法将数字证据定义为任何用计算机技术存储和传输的、支持犯罪行为如何发生的道理的数据。[2002]

6.3.2 数字证据在网络犯罪调查中的重要性

数字证据在网络犯罪调查的各个阶段发挥着重要的作用。通常分为两个主要阶段：[2003]调查阶段（确认相关证据、[2004]收集和保存证据、[2005]计算机技术和数字证据的分析）以及在法庭诉讼阶段展示和使用证据。

第一阶段与计算机取证有关，计算机取证将在后面的章节进行详细介绍。“计算机取证”这一术语描述的是对 IT 设备的系统分析，目的在于寻找证据。[2006] 以数字形式存储的数据数量的不断增长突出了调查过程中的逻辑问题。[2007] 可以使取证程序自动化（例如，通过例如对已知儿童色情图像进行基于哈希值的搜索 [2008] 或关键字搜索 [2009]）的方法在人工调查之外的调查工作中发挥着重要的作用。[2010] 计算机取证包括分析嫌疑人使用的硬件和软件 [2011]、恢复被删除的文件、[2012] 解密文件[2013] 或通过分析流量数据识别互联网用户等调查工作。[2014]

第二阶段关系到在法庭上展示数字证据。这一阶段与所要求的专门诉讼程序密切相关，因为数字信息只有通过使用计算机技术进行打印或显示后才能变得可见。

6.3.3 数字证据在传统犯罪调查中日益增长的重要性

调查人员寻找数据或捕获证据的能力以及法院处理数字证据的能力并不仅局限于网络犯罪调查。随着计算机技术在人民的日常生活中的不断融合，数字证据正在成为传统调查中很重要的证据来源。其中的一个实例是美国的一起谋杀案的审判过程，存储在嫌疑人的计算机内的搜索引擎请求记录被用于证明，在实施谋杀之前，嫌疑人频繁使用搜索引擎来寻找有关不可检测毒药的信息。

6.3.4 犯罪调查的新机遇

嫌疑人使用的信息通信技术和互联网服务，就会留下大量各种各样的数字痕迹，[2015] 例如，如果某一嫌疑人使用搜索引擎在网上寻找儿童色情资料，那么，其搜索请求、IP 地址有时甚至是其他的身份信息（如谷歌 ID）就会被记录下来。[2016] 在某些案件中，用于制作儿童色情资料的数码相机的文件中包括地理信息，如果这些图片在服务器上被捕获，就能使调查人员判定图片所拍摄的位置。[2017] 有时可以通过安装文件共享软件时生成的唯一 ID 号来追踪从文件共享网络上下载非法内容的嫌疑人。[2018] 篡改电子文件有可能产生元数据，这就使该文件的原作者能证明这种篡改行为。[2019]

经常被认为是优点的另一个方面是数字证据的中立性和可靠性。[2020] 与其他类型的证据（如，证人证词）相比，数字证据很少受到影响证据保存因素的影响。[2021]

6.3.5 面临的挑战

在计算机技术的早期，展开有关数字数据调查的执法能力受到了计算机取证设备和专门知识缺乏的限制。[2022] 电子证据日益增长的重要性衍生出很多计算机取证实验室。但是，这些数字证据的逻辑关联问题很少能轻易得到解决，这就留下了很多问题。

出现这些问题最根本的原因是，尽管数字证据与其他类型证据之间很多的相似性。但也还有较多的不同。某些一般原则 [2023] 仍旧适用，如，要求证据是真实的、完整的、可靠的 [2024] 和准确的，并且要求获取这类证据的过程符合法律程序等。[2025] 然而，除了相似性之外，还有很多方面使得数字证据具有唯一性，因此要求在犯罪调查中处理数字证据时要特别关注。

科学研究和训练的需求

数字证据是一种比较新颖的证据，这一领域的发展速度很快。尽管基础科学研究的时间框架非常有限，现在，需要在科学可靠的原则和程序上实施数字证据的搜索、检取和分析过程。[2026] 虽然现在已经开展了很多研究工作，但还有很多领域要求科学家密切关注。因此，证据的总体可靠性[2027] 或错误率的量化 [2028] 等有争议领域的科学研究仍应继续。不断进展的影响不会受限于对开展科学研究的需求。由于这种进展会在鉴定检验[2029]方面产生新的问题，所以，有必要不断培养专业人员。

对有约束力法律标准的需求

尽管计算机和网络技术已经在全球范围内得到了广泛的应用，但数字证据在法庭上的可接受性的问题确实类似的，即使在不同的法律体制下也是如此，处理数字证据的有约束力标准还没有广泛实施。[2030] 迄今为止，只有部分国家开始更新其相关法律，以便使法庭能够处理数字证据。[2031] 有关应对网络犯罪的实体刑法和诉讼条例在数字证据领域仍缺乏法律标准全球性的协调。

数量问题

如上所述，相对于存储物理文件，数字文件的低成本 [2032] 使其数量不断增加。[2033] 尽管所使用工具的能力使搜索过程 [2034] 实现了自动化，但在可以容纳数百万文件的存储设备中识别相关的数字证据对于调查人员而言是一个逻辑挑战。[2035]

专家报告的可靠性

分析和评估数字证据需要有专门的技能和技术理解，对法官、检察官和律师的教育过程中不需要涉及这些技能。因此，他们更多地依赖发现数字证据的专家的支持。[2036] 由于这种情况与 DNA 排序等其他复杂的调查技术没有明显的区别，它助长了针对这种依赖结果进行辩论的需求。为了避免负面影响，鼓励法院对证据提出质疑，并要求对有关的不确定性进行认定。[2037]

数字证据的脆弱性

数字数据非常脆弱，它很容易被删除 [2038] 或修改 [2039]，专家认为这是很令人担心的。[2040] 与其他类型的证据一样，数字数据表现出一定程度的不确定性。[2041] 为了避免出现对可靠性的不利影响，收集数字证据通常需要有一定的技术要求。例如，关闭计算机系统可以使存储在 RAM 系统内存 [2042] 中的数据全部丢失，除非使用特殊的技术手段来防止数据丢失。[2043] 如果数据存储在临时内存中，收集证据的技术可能与收集传统数字证据的过程有所不同。[2044] 这样一种复杂的方法是必要的，例如，如果嫌疑人正在使用加密技术，而调查人员试图检查信息是否存储在 RAM 内存中，这样的技术有助于调查人员获取加密了的信息。[2045]

修改数字证据有可能是犯罪人资故意而为或是调查人员无意而为。最不利情况下的数据丢失或修改可能会导致定罪错误。[2046]

由于其脆弱性，所以，计算机取证基本原则之一就是要保持数字证据的完整性。[2047] 在这种情况下，完整性可以定义为一种属性，凭借这种属性，从数字数据由授权来源生成、传输或存储的时间开始，数字数据不能以无授权的形式进行更改。[2048] 保护数字证据的完整性对保证可靠性和准确性是非常必要的。[2049] 处理这类证据要求有标准和程序，以便维护有效的质量体系。这包括很多方面，如案件记录、使用公认的技术和程序和只能由有资格的专家操作 [2050]，以及采用检验和、哈希算法和数字签名 [2051] 等特殊的方法等。所需的方法是有代价的，不能完全排除数据更改的风险。[2052]

所记录数据的有限性

很多互联网用户惊诧于有多少有关其行为的信息被存储下来。多数用户可能意识不到，当他访问互联网实施特殊行为（如，使用搜索引擎 [2053]）时，他已经留下了痕迹。这些痕迹在网络犯罪调查过程中可能是有用的数字证据来源。尽管如此，并非所有使用计算机技术过程中产生的信息都被存储下来。很多行为和信息，如，鼠标点击和键盘敲击就不被存储下来，除非安装了专门的监控软件。[2054]

提取的层次

虽然嫌疑人的行为会产生数字证据，这些证据与其所记录的事件被及时分开，因此这些证据更多的是历史记录而不是实时监测。[2055] 另外，证据没必要个人化。例如，如果嫌疑人使用互联网来获取儿童色情资料，他留下的痕迹不一定包含可以识别的身份信息。嫌疑人同时下载他的电子邮件或使用需要注册的服务就会产生一个链接。但由于这不属于必要的情况，所以专家指出，这有可能导致产生错误的提取层次。[2056]

对基础设施的要求

在有些国家，法庭设计数十年来甚至上百年来都遵循类似的原则。不考虑安全方面（如安装金属探测器或 X 光机）和舒适方面（如空调）的问题，在法庭诉讼过程中有可能用到一百多年前设计和布置好的法庭。[2057] 处理数字证据的需求产生的问题，即抽取层次和数字证据在没有打印机或显示器等工具的帮助下无法展示，给法庭设计带来了新的启示。[2058] 需要安装的显示器能够让法官、检察官、辩护律师、被告以及陪审团能够看到所展示的证据。安装和维护这类设备对司法系统产生了巨大的代价。

变化的技术环境

如上所述，技术在不断变化。这需要对诉讼程序和设备以及相关培训进行重新审视，目的在于确保调查的适用性和有效性。[2059] 随着操作系统版本和软件产品的不断更新，与调查有关的数据存储方式也在变化。硬件设备也在发生着同样的变化。[2060] 过去，数据存储在软盘中。今天，调查人员可能发现，相关信息可能存储在 MP3 播放器或带有 USB 存储设备的手表中。问题不仅仅是要与当今计算机技术的发展趋势保持一致。[2061] 鉴定专家也需要保留处理停用技术的设备，例如 5.25 英寸的软盘。除了硬件方面的变化，停用的软件也要能用：如果不使用原始软件，停用软件工具中的文件可能打不开。

也有必要用户行为的根本变化进行认真的研究。例如，宽带接入和远程存储服务器的使用已经影响了信息存储的方式。而在过去，调查人员能够集中注意嫌疑人的住所来寻找数字证据，今天，调查人员需要考虑的是，文件实际上有可能存储在国外，必要时，嫌疑人可以对文件进行远程读写。[2062] 云存储技术的逐渐应用为调查人员带来了新的挑战。[2063]

6.3.6 数字证据和传统证据的等效性

欧洲 2005 年和 2006 年开展的研究工作突出强调了 16 个被分析的国家的不同领域内数字证据和传统证据之间的等效性。[2064] 最常见的等效性是电子文件和纸质文件之间的等效性。常见的其他等效性有电子邮件和传统邮件、电子签名和传统手写签名以及电子公证证书和传统的公证证书。[2065]

6.3.7 数字证据和传统证据的关系

数字证据和传统证据间的关系可以通过两种方法加以区别：用数字证据替换传统证据，将数据证据用作补充传统证据（如，文件和目击证人）的附带原始资料。

用数字证据替换传统证据的一个实例是逐渐使用电子邮件取代传统信件。[2066] 如果没有发送物理信件，调查人员需要将注意力集中到数字证据上。这为分析方法和证据展示带来的新的启示。过去，手写信件是最为流行的非语言通信方式，法庭分析集中于当庭笔迹调查。[2067] 过去打字机普及时，鉴定专家所采用的方法已经从字迹鉴定转变为打字机分析。[2068] 随着从普通信件到电子邮件的

变化，调查人员转而需要处理电子邮件[2069]证据。[2070]虽然一方面其不能使用物理文件的结果限制了有关调查的可能性，但是另一方面，调查人员却可以使用工具实施自动电子邮件调查。[2071]

尽管大多数案件都涉及电子通信，而且重点仍在数字证据上，[2072]但其他类型的证据仍在识别违法者方面发挥着重要作用。这是相当有意义的，因为不是所有的计算机操作都会留下数字痕迹，而且并不是所有的痕迹都会联系到嫌疑人。[2073]使用公共互联网终端来下载儿童色情资料时，如果不进行注册[2074]或不留任何个人信息，可能很难将下载过程与嫌疑人联系起来。但如果可行，记录在视频监控器中的图像和留在键盘上的指纹是很有用的。相反，在指纹、DNA 痕迹和目击证人为主的传统犯罪中，数字证据可能是一种有价值的辅助证据来源。有关嫌疑人电话位置的信息可以使执法机构确认嫌疑人的位置，[2075]嫌疑人的搜索引擎请求可以帮助找到失踪受害人的位置。[2076]对于涉及金融交易的犯罪案件（例如儿童色情资料的商业交易[2077]），调查工作也可以包括金融机构保存的记录，以便确定违法者。2007 年，全球儿童色情资料调查就是根据与购买儿童色情资料有关的金融交易记录确定了嫌疑人。[2078]

6.3.8 数字证据的可接受性

对于数字证据，有两个主要方面值得讨论：收集数字证据的过程和数字证据在法庭上的可接受性。有关收集证据的特殊要求将在后续有关诉讼法的章节中进行进一步的讨论。对于数字证据的可接受性，尽管相对于传统证据有所不同，但基本原则是相同的。汇总这些原则是一个问题，这是因为不仅缺乏有约束力的国际协定，而且处理数字证据的教条式方法还有着本质的不同。虽然有些国家针对接收或拒绝数字证据给了法官很宽的裁决权，但其他国家已经开始制定法律框架来解决数字证据在法庭上的可接受性问题。[2079]

合法性

对传统类型的证据[2080]和类似的数字证据的可接受性的基本要求之一就是证据的合法性。[2081]这一原则要求数字证据的收集、分析、保存和最终在法庭上展示应当符合恰当的程序，并且没有侵害嫌疑人的基本权益。[2082]对收集、分析、保存和最终在法庭上展示证据的要求以及侵害嫌疑人权益的后果的要求，国家与国家之间各不相同。有可能违反原则和规则情况的范围可以从侵害嫌疑人的基本权益（如，隐私权[2083]）到不遵守诉讼要求。通常，由于法律不完善，有关证据的一般原则通常也会应用于数字证据。[2084]

针对收集数字证据的要求主要在刑事诉讼法中体现。例如，在大多数国家，对内容数据的截获要求有法院指令，而对远程设备的更大范围的搜索要求搜索人员位于同一国家。如果在没有法院指令的情况下进行截获，就会违反相应的程序，因而调查工作有可能侵害嫌疑人的权益。法律中通常不规定对保存证据的要求。[2085]但是，用于保护数字证据完整性的基本原则确实是一个指导方针。[2086]调查人员需要确定的是，证据从其在合法来源处产生、传输、或存储时起，没有以未授权的方式被改变。[2087]保护数字证据的完整性是必要的，这样可以确保其可靠性和准确性并且符合合法性的基本原则。[2088]法律中很少规定法院保存证据的程序。

如上所述，不仅要求发生了明显的变化，而且违反程序和侵害嫌疑人权益的情况也在发生显著地变化。[2089]有些国家认为，只有当证据是以侵害严重侵害嫌疑人权益（并非只违法正规的要求）的情况下收集的，则这样的证据才是不允许的，所以不排斥这类证据，其他国家，特别是那些采用毒树之果理论的国家，采用其他标准来衡量可接受性。[2090]

最佳证据规则

在习惯法的管辖范围内，最佳证据规则是非常重要的。[2091] 在很多陈年案件中有一些“最佳证据规则”的参考内容，“最佳证据规则”指的是按照习惯法的规定，只有最佳可用的待确定事实的证据才是被允许的。但无论是否曾经受欢迎，现在很少有当局再使用这条规则，有些执法当局甚至宣布这条规则废止。[2092]

当前的通用规则是，一条给定的证据是否是最佳可用的证据在于其影响分量，而非其可接受性。[2093]“基本证据规则”与最佳证据规则的关系紧密，该规则以前规定，在使用文件证据时，只有原件或者“备案”了的副本才允许用来证明其内容和真实性。但是，旧的规则实际上已经被法院抛弃，任何留存下来的规则在刑事诉讼过程中受到了立法的进一步的限制（现在，通常允许使用验证过的复印件。）[2094]

尽管现代技术对第一种方法中的弱点提出了异议，但要求在其可用之处使用原始文件而不依赖于可能不符合要求的副本或证人这一逻辑是很清楚的。[2095] 如果缺少最佳或基本文件证据是不可避免的，法院将接受辅助证据。辅助证据的存在说明还有其他或更好的证据。公文和司法文书通常用其副本来证明，不用考虑是否有原件；任何文件中所包含的叙述可以用验证过的文件副本来证明。[2096] 基本原则是减少抄写错误、证言误述文件内容以及未被察觉的篡改等风险。[2097] 严格的解释是：在原件丢失的情况下，该规则允许使用辅助证据（副本形式）。

这对于数字证据会产生很多问题，因而有必要确定原件。[2098] 由于数字数据通常可以在没有任何质量损失的情况下被复制，而在法庭上展示原始数据并不一定完全可行，最佳证据规则似乎与数字证据不相容。但法院已经针对新的发展趋势，开始通过同时接受电子复制品和原始文件的形式拓宽了规则的适用面。[2099] 在这种广义的解释中，最佳证据规则不再要求在每个案件中有书面的或证人的证言，但采用其内容的最佳可得证据。[2100] 此外，最佳证据规则已被大多数习惯法范围内建立的法定政权所采用。[2101]

传闻证据规则

传闻证据规则是另一基本原则，主要与习惯法国家有关。[2102] 传闻证据是一种由法庭外某个人陈述，由证人在法庭上给出的证据，试图用来证明陈述的真实性。[2103] 根据习惯法的规定，传闻证据通常不可接受纳；但在民事诉讼中，这一规则在英国已经被 1995 年的《民事证据法》废止，《民事证据法》规定，传闻证据的可接受性应当遵从法定的保护措施，并针对该规则保留了一定数量的习惯法例外。[2104]

根据习惯法传闻证据规则，除由诉讼过程中提供口头证据，试图作为其所声称的事实的证据的人所做的声明之外的其他声明都是不可接受纳的。[2105] 根据这一规则，庭外陈述指的是除证人在提供证据过程中做出的陈述之外的任何陈述，庭外陈述可以包括之前法律诉讼过程中提供的陈述。这样，该陈述可能是某个人未经宣誓所做的陈述或者是在誓言约束下口述的、书面的甚至是通过符号或手势的陈述，该人是否可以称为诉讼过程中的证人还存在疑义。[2106] 另外，该规则力图实现真实证人的交互询问，从而发现陈述中的问题。[2107]反之，具有个人知识的证人直接证明事实是有必要的。证人证言中不仅可以包含不可接受纳的证言，而且所展示的证据也可以包含不可接受纳的传闻。[2108] 已经有很多理由证明习惯法传闻证据规则的合法性，例如，传闻证据的潜在不可靠性有关的制造证据的危险。目前，处置传闻证据可接受性的规则当且仅当出于以下目的或目的之一才被采用，即法庭上做出陈述的人曾经造成另一个人相信该情况，或曾经造成另一个人在其所陈述的情况下采取行动或造成机器开始运行。[2109]

鉴于调查期间收集的数据（如日志文件）试图证明数字证据所声称情况自身的真相这一事实，在数字证据通常在法庭诉讼过程中是最为重要的证据类型的年代里，严格使用这一规则是有问题

的，某些习惯法国家已经针对传闻证据规则开始使用法定特殊情形。[2110] 由计算机、照相机或其他及其产生的、不带任何人的陈述的证据不属于传闻证据。[2111] 习惯法过去曾经保留这样的规定：视觉图像，即使是由人手拍摄产生，不属于对任何其所试图表达的事实的陈述，因此也不属于传闻证据。但现在有些规定却相反。[2112]

如果不存在法定的特殊情形，针对数字证据使用这一规则就出现了问题，有人指出，该规则只适用于由人所做的、包含声明的陈述。根据这一规则，无人干预的情况下由及其产生的信息不能视作潜在的传闻证据，[2113] 除非产生软件的过程被用作一种即使在那些情况下仍应用本规则的论据。[2114]

相关性与有效性

相关性与有效性是对数字证据可接受性的另外要求。[2115] 考虑到存储在私人计算机上的数据的数量，只有一少部分可能与案件有关，任何人都可以看出在网络犯罪调查过程中这一标准的重要意义。其应用对于限制证据收集和在法庭上展示证据两方面都很重要。不同于传统证据（在证据收集过程中，所有不相关的证据都被忽略），数字证据 [2116] 在其选择过程中面临着重重困难，因为当计算机硬件被捕获时，几乎不可能确定所关注的存储设备是否含有相关信息。

透明性

传统的传统搜索和捕获操作是公开实施的，因此可以保证嫌疑人能够意识到正在进行的调查工作，不同与此的是，实时通信监听工具之类的复杂调查工具不要求有类似的信息披露。尽管有技术能力，但并非所有国家都允许执法机构开展隐秘工作，或至少要求事后通知嫌疑人。收集、处理以及在法庭上使用证据的整个过程中的透明性为嫌疑人提供了对合法性和所收集证据的相关性提出质疑。

6.3.9 法律框架

如今，虽然很多国家都有涵盖大多数普通形式计算机犯罪的实体刑法条款，但对于数字证据而言，情况就有所不同。迄今为止，只有少数国家制定了专门针对数字证据的法律条款，另外，国际性有约束力的标准还很缺乏。[2117]

《关于电子证据的英联邦示范法》（2002）

2002 年，英联邦小型司法管辖区的司法部长决定建立一个工作组来针对电子证据制定示范法。研究小组的主要比较法分析结果是：对于数字证据的可接受性而言，产生数字证据的系统的可靠性要比证据文件本身更重要。以新加坡 [2118] 和加拿大 [2119] 法律为基础、2002 年开始实施的示范法 [2120]反映了这些研究成果，并且涵盖了很多数字证据对于习惯法国家的重要方面，例如，最佳证据规则 [2121] 的应用以及数字证据的完整性。

普通可接受性

3．在证据规则中，没有任何条款单纯凭借其是一种电子记录而否认其作为证据的可接受性。

第 3 节包含一条形式相似的法律框架的共同要素，如，1999 年《欧盟关于数字签名的指令》[2122]，该要素力图调节数字证据的各个方面。该条款旨在确保数字证据本身不属于不可接受的。在这方面，第 3 节规定了在法庭诉讼过程中使用数字证据的基础。但是，证据的可接受性并不

能单独保证，因为证据是数字的。对于数字证据而言，有必要符合有关证据的普通规则。如果证据是一种传闻，根据第 3 条，它就不能被采用。

法案的适用范围

4. (1) 除有关验证和最佳证据规则外，本法对有关记录的可接受性的习惯法或法律规则不做任何修改。

(2) 在使用任何有关记录的可接受性的习惯法或法律规则时，法院可以考虑本法所涉及的证据。

最佳证据规则的应用

6. (1) 按照(b)小节中的规定，最佳证据规则适用于电子记录，在任何法律程序中，证明记录和存储数据的电子记录系统完整性的过程要满足本规则的要求。

(2) 在任何法律程序中，如果打印形式的电子记录已经始终明显地发挥着作用或被信任或用作记录在打印品上的信息的记录，根据最佳证据规则，打印品就是记录本身。

如上所述，有些针对数字证据的标准与有关证据可接受性的传统原则有可能存在矛盾。这对于最佳证据规则而言尤为重要，尤其在习惯法国家具有极大的重要性。[2123] 最佳证据规则的目标是减少抄写错误、证言误述文件内容以及未被察觉的篡改等风险。[2124] 证据的可接受性要求文件证据是适用于涉案方的最佳证据。这条规则是否将数字证据本身排除在外是一个有争议的问题。[2125] 《英联邦电子证据示范法》第 4 节和第 6 节是法定特殊情形的一个实例。在这种情况下，都 4 节首先说明了示范法只是修改了有关验证和最佳证据的规则。根据这一总体说明，第 6 节修改了最佳证据规则，确保数字证据本身不是不可接受的。根据第 6 节的规定，数字证据不是不可接受的，因为最佳证据规则规定，产生数据的系统的完整性可以被证明。

《英联邦计算机及计算机相关犯罪示范法》（2002 年）

2002 年，《英联邦计算机与计算机相关犯罪示范法》草案问世。[2126] 除实体刑法条款和诉讼法律文本外，该草案还专门包含有关数字证据的条款。

证据

20. 在审理违法[颁布国]法律的违法案件中，下列事实：

(a) 断言干扰计算机系统的违法行为已经实施；

(b) 证据已经产生于该计算机系统；

其自身不能阻止该证据被接受

这一方法与《关于电子证据的英联邦示范法》（2002）第 3 条的专门条款类似。

6.4 管辖权

参考书目（节选）： *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004. *Hirst,* Jurisdiction and the Ambit of the Criminal Law, 2003; *Inazumi,* Universal Jurisdiction in Modern International Law, 2005; *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-

CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf; *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 69 et seq; *Sachdeva*, International Jurisdiction in Cyberspace: A Comparative Perspective, Computer and Telecommunications Law Review, 2007,, page 245 et seq; *Scassa/Currie*, New First Principles? Assessing the Internet's Challenges to Jurisdiction, Georgetown Journal of International Law, Vol. 42, 2001, page 117 et seq, available at: http://gjil.org/wp-content/uploads/archives/42.4/zsx00411001017.PDF; United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm; *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf; *Van Dervort*, International Law and Organizations: An Introduction, 1998; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

6.4.1 引言

网络犯罪是一种典型的跨国犯罪，涉及不同的司法管辖权。多个国家受到影响的情况并不罕见。违法者可能在 A 国采取行动，利用 B 国的互联网服务，而受害者则位于 C 国。这对刑事法的适用造成了挑战，[2127] 并且引发了哪些国家具有管辖权，哪些国家应推展调查工作，以及如何解决争议等诸多问题。虽然这种情况看起来已经颇为棘手，但仍有必要考虑在内的是，如果违法行为涉及云计算服务，则可能触发更多司法管辖权。[2128]

"管辖权"一词用于描述各种不同的法律问题。[2129] 根据国际公法的原则，"管辖权"系指某一主权国家管制特定行为的权力。[2130] 因此，管辖权是国家主权的一个方面。[2131] 然而，在网络犯罪方面，调查"管辖权"是指某一国家强制执行其国内法律的权力。[2132] 通常而言，如果该国具有管辖权，则执法工作将仅能执行一项调查。

6.4.2 不同的管辖权原则

不同的管辖权原则是可以区分的。

6.4.3 属地原则/客观属地原则

属地原则是最基本的原则和最常用的管辖权依据 [2133]。该原则适用于在某一主权国家领土内犯下的罪行 – 无论违法者或受害者的国籍如何。[2134] 一般管辖权只有在可以执行的情况下才有意义，并且法律的执行需要控制（通常限于其领土）这一事实说明了该原则的相关性。将属地原则编入计算机特定法律的做法之一是《欧洲理事会《网络犯罪公约》》第 22 条 1a 段。

第 22 条 – 管辖权
1　当根据本公约第 2 至 11 条确定的任何违法行为：
a　在任一缔约方领土内实施；
b　在悬挂该方国旗的船舶上实施；或者
c　在根据该方法律注册的航空器上实施；抑或

> *d* 由该方的一名国民实施时，并且如果违法行为可根据实施地点的刑法予以惩罚，或者如果违法行为是在任一国的属地管辖权以外实施的，则该缔约方须采取可能必要的此类立法及其它措施，确定对于上述违法行为的管辖权。
>
> *[…]*

该条款为计算机特定条款，因为它仅针对《网络犯罪公约》第 2 至 11 条所列违法行为。

然而，将其应用于网络犯罪案件时往往伴随着各种挑战。如果违法者和受害者实际身处某一国家内，并且违法者非法访问受害者的计算机系统，则毫无疑问已构成犯罪行为。但是如果违法者从国外采取行动，访问国内受害者的计算机系统，那么这种在领土以外实施的违法行为是否构成犯罪？

这些案件都具有治外法权元素。但是，国际法院在“莲花号（Lotus）”案件中明确指出，即使在各国仅在属地基础上应用管辖权的案件中，如果域外违法行为的构成元素之一（尤其是其效果）是在国内发生的，则仍可将该域外行为视为在境内实施的违法行为。[2135] 这一原则，亦称为“客观属地原则”，[2136] 在网络犯罪案件中具有重要意义。[2137]但是，考虑到违法者发出的恶意软件可能对各个国家的计算机系统造成影响，这就强调了这种广泛的属地定义容易造成潜在的管辖权冲突。[2138]如果违法者和受害者均不在该国内，并且犯罪行为的实施仅利用了该国的基础设施 – 例如，如果利用该国的电子邮件提供商发出含非法内容的电子邮件或者含非法内容的网站存储在位于该国的某一托管提供商的服务器上，若就此类案件应用属地原则，则潜在冲突的风险将进一步增加。

将这类广泛做法编入法典的示例之一是《2007 年新加坡计算机滥用法案》第 11(3)(b)节。

> **本法案规定的犯罪行为属地范围**
>
> *[…]*
>
> *11 — (1)* 根据第*(2)*款的规定，本法案的条款须对在新加坡以外及以内的任何个人具有效力，无论其国籍或公民身份如何。
>
> *(2)* 若任何人在新加坡以外的任何地点实施了本法案规定的违法行为，则可将其视为在新加坡内实施的违法行为予以处理。
>
> *(3)* 为实行本条的目的，如果相关违法行为中 –
>
> *(a)* 被告在案件审理相关期间在新加坡境内；或者
>
> *(b)*计算机、程序或数据在案件审理相关期间在新加坡境内，则本法案须适用。

这类广泛做法很可能导致对仅通过新加坡计算机系统传输的数据适用新加坡法律。[2139]

6.4.4 船旗国法原则

船旗国法原则与属地原则紧密相关，但将国内法律的应用延伸至航空器和船舶。考虑到水上和航空运输的互联网访问解决方案的可用性，[2140] 在一些案件中，违法者、受害者或受影响的计算机系统不在国家领土以内，而是位于领土边界以外的船舶或航空器上，这对刑法适用提出了诸多问题。

管理这类案件的方法示例之一是《欧洲理事会《网络犯罪公约》》第 22 条 1b 和 1c 段。

第 22 条 – 管辖权

1. 当根据本公约第 2 至 11 条确定的任何违法行为：

a 在任一缔约方领土内实施；

b 在悬挂该方国旗的船舶上实施；或者

c 在根据该方法律注册的航空器上实施；抑或

d 由该方的一名国民实施时，并且如果违法行为可根据实施地点的刑法予以惩罚，或者如果违法行为是在任一国的属地管辖权以外实施的，则该缔约方须采取可能必要的此类立法及其它措施，确定对于上述违法行为的管辖权。

[…]

6.4.5 效果原则/保护原则

效果原则旨在为外国国民在境外实施的犯罪行为（没有行为元素发生在领土内，但仍在领土内造成了重大影响）确定司法管辖权。[2141] 与之密切相关的是保护原则，为触发基本国家利益的类似案件确定司法管辖权。由于缺少违法者、受害者及所使用的基础设施这一事实，因此仅存在与某一国家的微弱联系，且该原则的应用饱受争议。[2142]

6.4.6 主动国籍原则

国籍原则系指针对海外国民的活动行使的司法管辖权。[2143] 这关系到国家规范其国民行为（不仅在其领土范围内，亦包括国外）的权力。相比于英美法系国家，这一原则在大陆法系国家内更为常见。[2144] 因此，英美法系国家倾向于通过对属地原则做出更为广泛的解释，弥补对基于国籍原则的管辖权的缺失。

由于与互联网相关的犯罪可以在不离开国家的情况下实施，因此在涉及网络犯罪案件时，该原则的相关性相对较低。然而，在生产儿童色情物品并通过计算机网络进行传播的情况下，该原则具有很强的针对性。[2145]

管理国籍原则的方法示例之一是《欧洲理事会《网络犯罪公约》》第 22 条 1d 段。

第 22 条 – 管辖权

1. 当根据本公约第 2 至 11 条确定的任何违法行为：

a 在任一缔约方领土内实施；

b 在悬挂该方国旗的船舶上实施；或者

c 在根据该方法律注册的航空器上实施；抑或

d 由该方的一名国民实施时，并且如果违法行为可根据实施地点的刑法予以惩罚，或者如果违法行为是在任一国的属地管辖权以外实施的，则该缔约方须采取可能必要的此类立法及其它措施，确定对于上述违法行为的管辖权。

[…].

6.4.6 被动国籍原则

被动国籍原则系指基于受害者的国籍的司法管辖权。考虑到与属地原则相重叠，该原则仅在国民在国外成为犯罪受害者时才具有相关性。该原则的应用一直饱受争议 [2146] – 尤其是因为它表明外国法律不足以保护外国公民 – 但是其接受程度在过去几十年内已经有所提升。[2147]

被动国籍原则法典化（非针对互联网）的示例之一是《德国刑法》第 7 节。

> ***第 7 节***
>
> 海外犯罪行为—其他案件
>
> *(1)* 德国刑法须适用于在海外针对德国实施的犯罪行为，如果该行为在实施地点属于犯罪行为，或者如果实施地点不受任何刑事管辖权管辖。

6.4.7 普遍性原则

普遍性原则确定与涉及国际社会利益的特定犯罪行为有关的司法管辖权。[2148] 该原则在严重犯罪行为（如危害人类罪和战争罪）方面尤为重要。[2149] 但是，承认这一原则的各个国家对其做出了进一步的规定。[2150] 因此，该原则在某些特定情况下甚至可以适用于网络犯罪。

可适用于网络犯罪案件的条款示例之一是《德国刑法》第 6(6)节。

> ***第 6 节***
>
> 侵害受国际保护的合法权益的国外犯罪行为
>
> 德国刑法须进一步适用于以下在德国境外实施的违法行为，无论实施当地的法律如何：
>
> *1* （已废除）；
>
> *2* 涉及第 307 节和第 *308(1)至(4)*节、第 *309(2)*节和第 *310* 节规定的核能源、爆炸物和放射物的违法行为；
>
> *3* 针对空中和水上交通的攻击（第 *316c* 节）；
>
> *4* 以性剥削、劳动剥削为目的的人口贩卖，以及协助人口贩卖（第 *232* 至 *233a* 节）；
>
> *5* 非法药品交易；
>
> *6* 第 *184a* 节、第 *184b (1)* 至*(3)*节和第 *184c (1)*至 *(3)*节，以及第 184d 节第 *1* 句规定的色情物品传播；
>
> *[...]*

根据第 6(6)节，德国可针对提供儿童色情内容下载的互联网网站行使管辖权，即使网站运营商位于德国以外，服务器不设在德国，并且没有德国互联网用户访问该网站。

6.5 程序法

参考书目（节选）： ABA International Guide to Combating Cybercrime, 2002; *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1; *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2; *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Galves*,

Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2; *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801; *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*; *Gercke/Tropina*, From Telecommunication Standardization to Cybercrime Harmonization, Computer Law Review International, 2009, Issue 5; *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002; *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3; *Houck/Siegel*, Fundamentals of Forensic Science, 2010; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008; *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004; *Menezes*, Handbook of Applied Cryptography, 1996; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004; *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12; *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970; *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf; *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005; *Vaciago*, Digital Evidence, 2012; *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1.

6.5.1 引言

正如上面各节所解释的那样，与网络犯罪作斗争，需要具备适当的实体刑法条款。[2151]至少在大陆法系国家中，如果没有这些法律，那么执法机构将无法调查犯罪行为。但在与网络犯罪作斗争的过程中，执法机构的要求不限于实体刑法条款。[2152] 为了完成调查 — 除了培训和装备 — 它们还需要一些程序手段，使执法机构能够采取必要的措施来查明违法者并收集刑事诉讼所需的证据。[2153] 这些措施可能与对那些与网络犯罪无关的犯罪进行调查所采取的措施是相同的 — 但鉴于以下事实，即违法者不必出现在犯罪现场，甚至不必接近犯罪现场，这就使得对网络犯罪的调查，很可能需要采取与传统犯罪调查不同的方式来进行。[2154]

之所以需要不同的调查方法，不仅仅是因为犯罪行为发生地和犯罪现场的独立性。在大多数情况下，正是上面提到的、执法机构所面临的众多挑战的结合，使得网络犯罪的调查显得很独特。[2155] 如果违法者在别的国家，[2156] 使用能够实现匿名通信的服务，并且，通过运用不同的公共互

联网终端来实施犯罪行为，那么对这种犯罪行为就很难仅仅通过诸如搜查和查封等传统的手段来进行调查了。为了避免误解，重要的是指出，对网络犯罪的调查既需要传统的侦查工作，也需要运用传统的调查手段 — 但网络犯罪调查还面临着一些无法仅通过传统调查手段就能解决的挑战。[2157]

有些国家已经采用了新的手段，使执法机构能够调查网络犯罪以及那些需要对计算机数据进行分析的传统犯罪。[2158] 在实体刑法方面是这种情况，《欧洲理事会关于网络犯罪的公约》包含一系列条款，反映了网络犯罪调查所需之程序手段方面的、被广泛接受的最低标准。[2159] 因此，以下内容将概述这一国际公约所提供的程序手段，此外还强调了一些该《公约》规定之外的国家方法。

6.5.2 计算机与国际互联网调查（计算机取证）

“计算机取证”一词用于描述为搜寻数字证据而进行的系统性数据收集和计算机技术分析工作。[2160] 这类分析通常在犯罪行为发生以后进行。[2161] 因此，它是计算机犯罪和网络犯罪调查的主要部分之一。执行此类调查的调查人员会面对若干挑战，第 3 章将详细阐述这些挑战。

计算机取证中专家的可能参与程度展示了其在调查过程中的重要性。此外，互联网调查的成功对于取证资源可用性的依赖程度突显了在此领域开展培训的需要。只有在调查人员接受过计算机取证培训，或者可以获取该领域内专家资源的情况下，才可以针对网络犯罪执行有效的调查和起诉工作。

定义

目前存在多个“计算机取证”定义。[2162] 它可以定义为“对信息技术设备和系统进行检查，以便为刑事或民事调查获取信息”。[2163] 在实施犯罪时，嫌疑人会留下一些蛛丝马迹。[2164] 这种表述在传统犯罪调查和计算机犯罪调查中都是有效的。传统犯罪的调查与网络犯罪的调查之间主要的区别在于以下事实，即网络犯罪调查一般需要一些与数据有关的特殊调查技术，并且可以通过专用的软件工具来帮助调查。[2165] 除了适当的程序手段，进行此类分析还要求主管部门具备管理和分析相关数据的能力。取决于违法行为和涉及的计算机技术，在程序调查工具和取证分析技术方面的要求通常各不相同，[2166] 常常伴随着一些独特的挑战。[2167]

取证调查的各个阶段

一般可以将取证调查过程分为两个主要阶段：[2168] 调查阶段（鉴定相关证据[2169]、收集和保存证据、[2170] 分析计算机技术和数字证据）和在法庭诉讼中提供、使用证据阶段。为对各种不同的活动进行说明，以下章节将这一模型扩展至四个阶段进行讨论。

证据鉴定程序

日益增加的硬盘容量 [2171] 以及数字文件存储相对于实体文件存储的、不断降低的成本 [2172] 促使数字文件的数量稳步增长。[2173] 鉴于有必要将调查重点放在相关证据上，以防止出现不予受理的情况，必须特别注意证据的鉴定工作。[2174] 因此，取证专家在设计调查战略和选择相关证据时发挥着重要作用。例如，他们可以确定相关证据在大存储系统上的位置。这使得调查人员可以将调查范围限定在与调查工作相关的那些计算机基础设施部分，避免对计算机硬件实施不适当的大规模查收。[2175] 由于存在各种类型的存储设备，导致很难确定相关证据的存储位置，因此这种选择程序就非常重要。[2176] 在犯罪嫌疑人没有在本地存储信息，而是使用远程存储手段时，这一过程尤其有效。宽带接入和远程存储服务器的可用性影响了信息存储的方式。如果犯罪嫌疑人将信息存储在位于另一国家内的服务器，这一简单的动作可以使得查找证据的工作更加困难。在这种情况下，取证分析可用于确定是否使用了远程存储服务。[2177] 相关数字信息的确定并不限于文件本身。操作系统

提供用于快速确定文件的软件工具数据库可能也包含相关信息。[2178] 即使系统生成的临时文件也可能包含用于刑事诉讼程序的证据。[2179]

另一个证据鉴定的示例是取证专家参与确定正确的程序性手段。许多国家允许执法机构执行两类实时观察 – 实时收集流量数据和实时截获内容数据。通常而言，内容数据的截获较流量数据的收集更具侵扰性。取证专家可以确定流量数据的收集是否足以证明实施了一项犯罪行为，因此有助于调查人员在收集有效证据的需求和通过从一组效果等同的方案中选择强度最低的手段来保护犯罪嫌疑人权利的义务之间达成正确的平衡。两个示例均表明，取证调查人员的职责并不限于调查的技术方面，还包括保护犯罪嫌疑人基本权利的责任，从而避免出现对所收集的证据不予受理的情况。[2180]

证据的收集和保全

参与数字证据的收集需要具备复杂的技能，因为用于收集存储在家用计算机硬盘上的证据的技术与用于截取数据传输过程的技术之间存在巨大差异。尤其是涉及高水平违法者时，调查人员常常面对需要迅速做出决定的情况。其中一个示例是，是否应关闭一个正在运行的计算机系统，以及如何执行这一程序。为避免对相关数字证据的完整性造成干扰，一个常见的指令是拔出插头，因为这样可以阻止文件发生任何更改。[2181] 然而，这样的能源中断可以激活加密，[2182] 并因此阻止访问已存储的数据。[2183] 首批响应者，即执行第一个步骤收集数字证据的人，对于整个调查过程负有重大责任，这是因为任何的错误决定均可对保全相关证据的能力产生重大影响。[2184] 如果他们做出了错误的保全决定，则可能丢失重要的踪迹。

取证专家需要确保确定所有相关证据。[2185] 如果违法者将文件藏在一个存储设备中，以阻止执法机构对文件内容进行分析，这会为取证专家的工作造成困难。取证调查可以确定隐藏文件，并使其成为可访问的文件。[2186] 如果数字信息已被删除，则有必要执行类似的恢复程序。[2187]通过简单地放置在虚拟回收站进行删除的文件并不能阻止执法机构获取它们，使用专用的取证软件工具即可恢复这类文件。[2188] 然而，如果违法者使用了某种工具，确保通过覆写信息的方式安全删除文件，则通常不可能进行恢复。[2189] 如果违法者试图通过使用加密技术阻止对相关信息的访问，则也可为证据收集带来一定的困难。对这类技术的使用愈加频繁。[2190] 鉴于这样可以阻止执法机构访问和审查加密信息，加密技术的使用为执法机构的工作造成了重大挑战。[2191] 取证专家可试图对加密文件进行解密。[2192] 如果不可能进行解密，他们可通过制定可访问加密文件战略（例如使用键盘记录程序），为执法机构提供支持。[2193]

证据收集的参与包括评估和实施新的工具。新方法的示例之一是关于远程取证工具的辩论。[2194] 远程取证工具使得调查人员能够在犯罪嫌疑人不知道自己系统被调查的情况下，远程、实时地收集证据，[2195] 或者远程监控犯罪嫌疑人的活动 [2196]。在这类工具可用时，它可以在制定收集数字证据战略中发挥一定作用。

与服务提供商之间的沟通

由于大多数用户利用互联网服务提供商（ISP）的服务访问互联网或存储网站，因此他们在众多网络犯罪调查中发挥着重要作用。在许多情况下，互联网服务提供商拥有侦查并防止犯罪行为，以及为执法机构的调查工作提供支持的技术能力，这一事实促进了对于互联网服务提供商在网络犯罪调查中的作用的激烈辩论。所讨论的义务包括从强制性执行预防技术到自愿为调查工作提供支持。[2197] 取证专家亦可通过准备提交给服务提供商的请求 [2198] 和协助调查人员制作充分的案例历史[2199] （证明所收集的证据可靠性时必不可少），为调查工作提供支持。在此类调查中，执法机构与互联网服务提供商之间的合作需要应用特定的程序。[2200] 欧洲理事会关于执法机构和互联网服务提供商开展合作的指导原则 [2201] 中包含了一系列基本程序，其中包括提供有关调查技术的解释和协助[2202] 以及优先顺序等问题，[2203] 取证专家的协助在此方面非常有用，可提高各项程序的效率。

与互联网服务提供商开展的紧密合作在查明犯罪嫌疑人方面尤其重要。网络犯罪嫌疑人总会留下蛛丝马迹。[2204] 流量数据分析（如审查互联网服务提供商保存的日志文件）可引导调查人员查明违法者用于登录互联网的连接。[2205] 违法者可以通过使用匿名通信技术，试图阻碍调查人员的工作。[2206] 但即使在这种情况下，如果调查人员和互联网服务提供商紧密合作，调查仍然可以进行。[2207] 其中一个示例是取证工具 CIPAV（计算机和互联网协议地址验证工具），在美国曾用于查明犯罪嫌疑人是否使用了匿名通信服务。[2208] 互联网服务提供商和调查人员之间合作的另一个示例是电子邮件调查。电子邮件已成为了一种非常流行的通信手段。[2209] 为躲避调查，违法者有时会使用免费的电子邮件 地址，这样他们可以使用伪造的个人信息进行注册。然而，即使这样，对于电子邮件提供商的报头信息 [2210] 和日志文件的审查会在某些情况下促使查明犯罪嫌疑人。

与提供商进行合作和沟通的必要性不仅限于互联网服务提供商。由于某些犯罪行为，如网络钓鱼 [2211] 和儿童色情内容的商业性传播，都包括金融交易，因此查明违法者身份战略之一是从这类交易中涉及的金融机构处获取数据。[2212] 例如，在德国开展的一项调查根据信用卡记录查明了一批从商业性网站上下载儿童色情内容的违法者。根据调查人员的请求，信用卡公司分析了他们的客户记录，查明了曾使用他们的信用卡在特定网站上购买儿童色情内容的客户。[2213] 但在违法者使用匿名支付方法时，这类调查工作会更加困难。[2214]

信息通信技术的检查

大多数调查的第一步是证实违法者是否具备实施犯罪的能力。鉴定专家的主要任务之一是检查所捕获的硬件和软件。[2215] 这类检查可以在搜查嫌疑人住所 [2216] 的现场进行，也可以在捕获售后进行。为了开展这类调查，首要责任人通常捕获所有的相关存储设备——每个存储设备有可能保存有数百万的文件，者通常会给调查人员带来逻辑挑战。[2217] 前述的相关性和有效性原则对数字证据的可采用性意义重大。[2218] 因此，确认和选择有关犯罪行为的硬件是调查期间的主要任务之一。[2219]

例如，对可用硬件组件的分析能够证明嫌疑人的计算机能够实施拒绝服务攻击 [2220] 或装有防止操纵操作系统的芯片。硬件分析对于确定嫌疑人的过程也是非常必要的。有些操作系统能够在安装过程中分析计算机系统的硬件配置，并将其上传给软件制造商。如果可以根据来自软件公司的信息来检测嫌疑人的硬件配置，那么硬件分析就有助于检验所捕获的计算机系统是否符合条件。大多数操作系统都会在运行期间保留一份存放在计算机系统内的硬件日志。[2221] 根据日志文件中 Windows 注册表之类的记录，鉴定人员可以确定过去使用过但在搜查和捕获过程中没有使用的硬件。

除硬件分析外，软件分析也是网络犯罪调查中的常规任务。计算机软件对于计算机系统的运行时必要的。出操作系统外，其他软件工具可以使计算机系统按照用户的要求运行。鉴定专家可以分析软件工具的运行情况，目的是证明嫌疑人有能力实施特定的犯罪行为。例如，调查人员可以调查嫌疑人的计算机是否装有能够在图片中加密数据的软件（隐写 [2222]）。安装在嫌疑人计算机内的软件工具的详细记录也可以有助于进一步设计调查战略。例如，如果调查人员发现用于安全删除文件的加密软件，他们可以专门搜索加密了的或删除了的证据。[2223] 调查人员还可以确定计算机病毒或其他形式的恶意软件的功能，并重构软件运行过程。[2224] 在有些情况下，当发现嫌疑人的计算机内有非法内容时，嫌疑人可以声称没有下载文件，一定是计算机病毒所为。在这样的情况下，取证调查可以设法识别安装在计算机系统内的恶意软件并确定其功能。如果计算机系统已经僵尸网络 [2225] 被感染或已经成为僵尸网络的一部分，也可以开展类似的调查。此外，软件分析对于确定一种软件是仅为实施犯罪而设计还是出于合法或非法的目的（双重应用）而设计也很重要。这种差别是相当重要的，因此某些国家对生产非法设备的罪行认定只限于专门或主要为施犯罪行为而设计的非法设备。[2226]

与数据有关的调查不仅限于对软件功能的调查，还包括 pdf 文件、视频文件等不可执行文件的分析。这些嫌疑人计算机的调查所涉及的范围从特定文件的内容搜索到针对文本文件的自动关键词搜索 [2227] 以及对已知图像的搜索。[2228] 文件分析还包括对可能已经伪造了的数字文件 [2229] 的检查和对

元数据的调查。[2230] 这类分析可以确定文件最后一次被打开或修改的时间 [2231]。[2232] 此外，元数据分析可用于确认含有恐吓信息的文件的作者，或者是用于制作儿童色情图像的相机的序列号。也可以根据语言学分析确认作者，这有助于决定嫌疑人之前是否也写过文章，并有助于在这种情况下识别其身份信息。[2233]

跟踪与报告

数字证据的一个最大问题就是它非常脆弱，可以相当轻易地被删除 [2234] 或修改。[2235] 如上所述，数字证据的脆弱性带来的结果就是需要保持其完整性。[2236] 因此需要有个案记录。如果涉及鉴定专家，有资格的专家 [2237] 参与制作个案记录是保持数字证据完整性的一种方法。[2238] 但是，如果不可能查封硬件或不活的硬件数量很少时，也需要鉴定专家的参与。在这些情况下，有些国家授权调查人员对文件进行复制。这就需要特别关注保护复制文件的完整性，防止其在复制过程中出现各种各样的更改。[2239]

在法庭展示证据

一般来说，调查工作的最后一个阶段就是在法庭上展示证据虽然在法庭上展示证据通常由检方律师和辩护律师完成，但鉴定专家可以在刑事诉讼过程中发挥重要的作用，他作为专家见证人可以帮助涉案人员了解证据产生的过程以及用于收集和评价证据的程序等信息。[2240] 随着数字证据越来越复杂，对鉴定专家的需求也在增加，这将增加法官、陪审团、检察官和辩护律师对专家报告的信任度。[2241]

法院的检查操作

虽然计算机取证在很大程度上取决于计算机硬件和计算机数据，但通常不一定需要自动操作，因而计算机取证在很大程度上还需要保留人工操作。[2242] 尤其在制定调查战略在搜查和检取过程中搜索可能的证据方面的情况确是如此。这样的人工操作所需要的时间和违法者自动实施攻击的能力是执法机构面临的最大问题，尤其是对大量嫌疑人和大量数据进行的调查的过程中更是如此。[2243] 但是有些过程，如，搜索可能的关键词或恢复被删除的文件，都可以使用专门的鉴定分析工具自动完成。[2244]

6.5.3 安全保障

几年前，世界范围的执法机构已经强调过对足够多的调查工具的迫切需要。[2245] 考虑到这一问题，涉及诉讼工具的欧洲理事会《网络犯罪公约》遭到批评确实令人感到意外。[2246] 这些批评主要集中在一个方面，即《网络犯罪公约》包含大量的关于使用调查工具的条款（第 16-21 条），但只有一个条款（第 15 条）涉及安全保护。[2247] 另外还需注意的是，不同于《网络犯罪公约》中的实体刑法，在国家范围内对实行《网络犯罪公约》进行的调整几乎是不可能的。[2248] 批评的重点主要集中在数量方面。《网络犯罪公约》遵循安全保护的集中控制而不是将其针对于个别工具的观念是正确的。但这不一定意味着弱化了对嫌疑人权益的保护。

欧洲理事会《网络犯罪公约》最初是作为一种国际框架和对抗网络犯罪的工具而设计的，并不仅限于欧洲理事会成员国。[2249] 讨论诉讼工具的必要性时，《网络犯罪公约》的起草者（包括美国、日本等非欧洲国家的代表）认识到现有有关保障的国家方法，特别是各种刑法体系下保护嫌疑人权益的方式差别非常大，有可能无法为所有的成员国提供详细的解决方案。[2250] 因此，《网络犯罪公约》的起草者决定《公约》文本中不包含具体的规定，但要求成员国使用基本点国家和国际保障标准。[2251]

第 15 条——条件与保障

1. 各方应确保本节所规定权力的建立、实施和应用应符合其国内法律规定的条件和保障要求，即应对人权、自由进行保护，包括 1950 年《欧洲保护人员和基本自由公约》、1996 年《联合国公民权利和政治权利国际公约》以及其他适用的国际人权法律条文所规定的享有的权利和承担的义务，同时还要遵循合理性原则。

2. 这样的条件和安全保护应包括司法或其他的独立监督、合理判定的依据以及这类权力和诉讼程序的范围和期限的限制，尤其要考虑诉讼程序和权力的特点。

3. 就符合公众利益而言，特别是良好的司法行政，各方应考虑本节所涵盖的权利和诉讼程序对第三方的权利、责任和合法权益的影响。

第 15 条的原则依据是个签约国应采用其国内法律现有的条件和保障。如果法律能提供适用于所有调查工具的核心标准，这些原则也应适用于有关互联网的法律条款。[2252] 如果国内法律不是以对保障和条件的集中管理为基础，那就有必要对相当于有关互联网法律条款的传统法律条款下实施的保障和条件进行分析。

但是《网络犯罪公约》并不单单涉及国内立法中现有的保障。对应用要求的不同表现为协调工作的积极方面可能不再适用，这有可能存在缺陷。为了保证有不同法律传统和安全保障的签约国能是当地执行某些标准，[2253] 欧洲理事会《网络犯罪公约》通过参考基本法律框架（如，1950 年的《欧洲理事会保护人权公约》、1966 年的《联合国有关公民权利和政治权利公约》以及其他适用的国际人权法律文书）定义了最低标准，

由于《网络犯罪公约》还可以由不属于欧洲理事会成员的国家 [2254] 签字批准，所以，有必要强调的是，在评价非欧洲理事会《网络犯罪公约》成员签约国的安全保障系统时，不仅要考虑《联合国公民权利和政治权利国际公约》，还要考虑《欧洲理事会人权和基本自由保护公约》。

对于网络犯罪的调查工作，欧洲理事会《网络犯罪公约》第 15 条中最重要的一个条款是参照《欧洲人员公约》第 8 条第 2 款制定的。

第 8 条

1. 任何人有权尊重其个人和家庭生活、住宅和通信。

2. 为了防止混乱或犯罪、为了保护健康或道德，或为了保护其他人的权利和自由，政府当局不应对符合法律的、公共安全民主社会中国家安全利益、公共安全和国家福利所必要的权利进行干涉。

欧洲人权法院已经作出努力，试图定义更多有关管理电子调查，尤其是监视，的准确标准。如今，判例法已经成为有关通信调查的国际标准中最重要的资源之一。[2255] 判例法尤其注意到了调查干扰的严重性 [2256]、目的 [2257] 和合理性。[2258] 判例法的基本原则是：对调查工具法律依据的充分性的需求、[2259] 对法律依据的主题必须明确的要求、[2260] 可需要预先了解的执法机构的能力 [2261] 以及对通信监视只有在严重犯罪情况下才合法。[2262]

除此之外，欧洲理事会《网络犯罪公约》第 15 条第 2 段考虑到了合理性原则。[2263] 这一条款对非欧洲理事会成员的签约国尤其重要。如果现有国家安全保障制度不足以保护嫌疑人，成员国必须在批准和实施过程中制定必要的安全保障制度 。

最后，欧洲理事会《网络犯罪公约》第 15 条第 2 分款明确提到了一些相关安全保障措施，[2264] 包括监督、证据证明申请以及对诉讼程序范围和期限的限制。

与以上提到的基本原则不同，这里的安全保障方法不一定需要用任何工具来实施，只有在符合所涉及诉讼程序的特点的情况下才能使用工具。究竟属于哪一种情况需要由国家立法机关决定。[2265]

欧洲理事会《网络犯罪公约》规定的有关安全保障体系的一个重要方面是，执法机构灵活使用工具的能力以及保证有效的安全措施取决于分级安全保障体系的实现。《网络犯罪公约》没有明确反对各成员国对所有的工具采用相同的安全保障措施（如，法院判令的要求），但这样一种方法会影响到执法机构的灵活性。在分级安全保障体系中充分保护嫌疑人权益的能力主要取决于调查工具的潜在影响和相关安全保障之间的折中。为实现这一目标，有必要对较小密集工具和较大密集工具进行区分。欧洲理事会《网络犯罪公约》中有很多这样的区分实例，它能使各签约方进一步制定分级安全保障体系，包括以下内容：数据内容截获（第 21 条）[2266] 和流量数据收集（第 20 条）[2267] 的区别。与收集流量数据不同，内容数据截获仅限于严重犯罪。[2268] 要求快速保存已存储的计算机数据（第 16 条）[2269] 与按照要求（第 18 条）[2270] 提供已保存计算机数据的区别。第 16 条只能使执法机构提出保存数据，而不是披露数据的要求。[2271] 第 18 条中，负责提交“用户信息”[2272] 与负责提交“计算机数据”[2273] 的区别。[2274]

如果正确评价调查工具的密集程度以及对嫌疑人潜在的影响，并且所设计的安全保障体系与分析的结果一致，分级安全保障体系不会导致形成不平衡的诉讼工具体系。

6.5.4 已存储计算机数据的快速保存和披露（速冻程序）

确定一名实施网络犯罪的违法者通常要求对流量数据的分析。[2275] 尤其是 IP 地址可以帮助执法机构对违法者进行回溯跟踪。只要执法机构获得了流量数据，在某些情况下甚至有可能确定使用不需要身份认证的公共互联网终端的违法者。[2276]

调查人员所面临的主要困难是，有关问题信息的流量数据提出在相当短的时间内被自动删除。这类自动删除的原因是，一个过程（如发送一封电子邮件、访问互联网或下载电影）结束后，流量数据是在过程发生期间产生的，并且能使运行的过程不再被需要。从电子学的角度看，大多数互联网服务提供商通常热衷于对于尽快删除信息，因为长期存储数据需要更大（昂贵）的存储容量。[2277]

但是，经济方面的考虑并不是执法机构快速完成调查工作的唯一原因。某些国家拥有严格的法律来禁止在过程结束后存储特定的流量数据。《欧盟关于隐私和电子通信的指令》第 6 条就是这类限制的一个实例。[2278]

第 6 条——流量数据

1. 有关用户和使用者、由公共通信网络或公用电信服务提供商所拥有的流量数据如果不再用于通信传输，则在不影响本条 2、3、5 款和第 15 条第（1）款的情况下必须被删除或使其无意义。

2. 用于用户计费和互联付款所需要的流量数据可以被处理。这类处理操作只有在账单已被依法质询或有后续付款时才能被接受。

因此，时间就成了调查人员最关键的问题。一般来说，由于在犯罪准备、发现犯罪和通知执法机构过程中有些时间有可能会流逝，所以这对防止有关数据在长时间的调查过程中被删除的实施机制是很重要的。因此，人们现在正在讨论两种不同的方法，即数据保留和数据保管（“速冻程序）。[2279]

数据保留义务强制要求互联网提供商保存一段时间的流量数据。[2280] 在最新的立法途径中，需要保存的记录长达 24 个月。[2281] 这将能使执法机构得到确定违法者所需的必要数据，即使违法者经历了长达一个月的犯罪准备。[2282] 最近，欧洲议会 [2283] 最近采纳了数据保留义务，并且当前正在美国进行讨论.[2284] 有关数据保留的原则问题，在下面的内中将对此作出介绍。

《网络犯罪公约》

数据保存是另一种确保网络犯罪调查不因在长时间的调查过程中数据被删除而造成失败的方法。[2285] 根据数据保存法，执法机构可以要求服务提供商防止删除特定数据。计算机数据的快速保存是一种工具，该工具能使执法机构立即作出反应 ，以避免在长时间的过程中发生大问题。[2286]《网络犯罪公约》的起草者决定采用数据保存而不是数据保留。[2287] 具体规则在《公约》的第 16 条中给出。

第 16 条– 已存储计算机数据的快速保存

1. 各方应采取必要的法律和其他措施，使其主管部门能够索取或获得快速保存的特定的、已经利用计算机系统进行存储了的计算机数据（包括流量数据），当有理由相信这些计算机数据数据极易丢失或被修改时尤为如此。
2. 当签约方以要求某人在其控制范围内保存特定的已存储计算机数据的方式实施了上述第 1 款的要求时，该签约方应采取必要的法律和措施，责成该人在必要的期限内保存并维护该计算机数据的完整性，最长时间为 90 天，以确保主管部门能对信息进行披露。签约方可以对该要求进行后续更新。
3. 签约方应采取必要的法律和其他措施责成负责保存计算机数据机密性的保管人或其他人员在其国家法律规定的期限内履行上述程序。
4. 本条所涉及的权力和程序应当遵从第 14 条和第 15 条的规定。

从互联网服务提供商的角度看，与数据保留相比，对数据保存的限制条款比较宽松。[2288] 互联网服务提供商不需要为所有的用户保存所有的数据，但必须保证特定数据在计算机主管部门索取时不被删除。数据保存有很多优点，它不仅涉及提供商层面上的保存，而且涉及数据保护层面上的保存。保存来自数以百万计的互联网用户的数据是没有必要的，只有那些有关犯罪调查中的嫌疑人的数据才予以保存。然而，有必要指出的是，对实施犯罪后立即删除的数据而言，数据保留就会体现出优势。在这种情况下，不同于数据保留职责，数据保存要求可能不会保护相关数据被删除。

依照第 1 条提出的要求责成提供商在其收到要求函时保存已由其处理过的并且没有被删除的数据。[2289] 并没有局限于流量数据，因为流量数据只是一个具体实例。第 16 条不强制提供商开始收集有可能非正常存储的信息。[2290] 另外，第 16 条没有责成提供商向有关部门传送相关数据。该条款仅授权执法机构防止有关数据的删除，而不保证提供商传输该数据。数据传送的职责在欧洲理事会《网络犯罪公约》第 17 条和 18 条中加以规定。将数据保存的职责与数据披露的职责分开的优点在于，对履行两类职责的条件有可能不同。[2291] 从即时反应的重要性的角度看，这有可能支持不使用法官裁令的要求，从而使检方或警察能够提出对数据进行保存的要求。[2292] 这有可能使主管部门的的反应更迅速。这样就可以通过要求披露数据的法官裁令来保护嫌疑人的权益。[2293]

欧洲理事会《网络犯罪公约》第 18 条的其他方面给出了披露已保存数据有关规定：

第 18 条——制作订单

1. 各方应采取必要的法律和其他措施，使其主管部门有权要求：
   a. 在签约国范围内的某人在其所拥有或控制的范围内提供存储在计算机系统或计算机数据存储介质中的计算机数据；
   b. 在签约国范围内提供其服务的服务提供商在其所拥有或控制的范围内提供与这类服务有关的用户信息。
2. 本条所涉及的权力和程序应当遵从第 14 条和第 15 条的规定。
3. 在本条中，术语“用户信息”系指包含在计算机数据或服务提供商所拥有的其他（除流量或内容数据之外）的数据中且与其服务用户有关的信息，以及该信息赖以存在的下列信息：
   a. 所使用的通信服务的类型、所采取的技术以及服务的期限；
   b. 用户的身份信息、邮政或地理地址、电话和其他访问号码、服务协议或约定下的账单和付款信息；
   c. 在服务协议或约定下安装通信设备现场的其他任何信息。

根据欧洲理事会《网络犯罪公约》第 18 条第 1.a 段的规定，可以责成已经保存了数据的提供商披露该数据。

《网络犯罪公约》第 18 条不仅适用于《公约》第 16 条所规定的数据保存指令发出后的情形。[2294] 该条款是一条执法机构能使用的一般条款。如果制作订单的接收者自愿传送所要求的数据，不限制执法机构查封硬件，但可以采用更为宽松的制作订单。与实际查封硬件相比，要求提供有关信息的指令通常比较宽松。因此，该条款尤其适用于取证调查不要求接触到硬件的情形。

除了提交计算机数据的职责外，欧洲理事会《网络犯罪公约》第 18 条使执法机构能够下达提交用户信息的指令。这一调查条款对于基于 IP 地址的调查非常重要。如果执法机构能确定违法者实施犯罪时所使用的 IP 地址，就需要确定实施犯罪行为时使用该 IP 地址的人。[2295] 根据《网络犯罪公约》第 18 条第 1.b 段的规定，提供商应提交第 18 条第 3 段所列的用户信息。[2296]

当执法机构通过路径回溯追踪违法者，并需要立即访问以确定通信传输的路径时，第 17 条授权其要求快速披露部分流量数据。

第 17 条——快速保存和部分披露流量数据

1. 对于第 16 条要求保存的流量数据，各方应采取必要的措施，以便：
   a. 确保快速保存流量数据可行，不论是否有几个服务提供商涉及到信息传输；
   b. 确保向签约方的主管部门或该部门指派的人员快速披露数据，以便使签约方确定服务提供商以及通信的传输路径。
2. 本条所涉及的权力和程序应当遵从第 14 条和第 15 条的规定。

如上所述，《网络犯罪公约》严格区分了按照要求保存数据的职责和向主管部门披露数据的职责。[2297] 第 17 条给出了明确的分类，因为它将确保涉及数个服务提供商时流量数据的保存职责与披露确定传输路径所需信息的职责结合在一起。如果没有部分披露这样的举措，在某些情况下，如果涉及多个提供商，执法机构有可能无法回溯追踪到违法者。[2298] 由于将两种以不同形式影响嫌疑人权益的职责结合在一起，这就有必要讨论本条款所涉及的安全保障的关键问题。

《英联邦计算机与计算机相关犯罪示范法》

2002 年的《英联邦示范法》有类似的方法。[2299]

条款

数据的产生

15 在警察提出申请的基础上，如果地方法官认为指定的计算机数据、数据的打印输出或其他信息是出于犯罪调查或刑事诉讼的目的而被合理使用，该地方法官可以要求：

(a) [颁布国]领土范围内控制计算机系统的人从其计算机系统中产生出指定的计算机数据、数据的打印输出或该数据的其他可理解的输出；

(b) [颁布国]领土范围内的互联网服务提供商准备有关订购或使用其服务的人的信息；

(c) [2300] [颁布国]领土范围内已进入指定计算机系统的人在其计算机系统中处理、编辑指定的计算机数据并将这些数据提供给指定的人。

存储流量数据的披露

16[2301]如果警察认为存储在某计算机系统中的数据是出于犯罪调查的目的而被合理使用，该警察可以通过书面通知的形式，要求控制计算机系统的人披露有关指定通信的流量数据，以便确定：

(a) 服务提供商；

(b) 通信传输的路径。

数据保存

17 (1) 如果警察认为：

(a) 存储在计算机系统中的数据是出于犯罪调查的目的而是用的；

(b) 如果该数据被破坏或变得不可用，则存在风险；

该警察可以通过书面通知的形式，要求控制计算机系统的人确保通知中指定数据的保存期限达到通知中规定的时间，但不得超过七天。

(2) 如果[法官][地方法官]批准保存期限超过规定的时限，则在单方申请的条件下，保存期限可以超过 7 天。

6.5.5 数据保留

数据保留职责强制要求互联网服务提供商要保留一定时期的流量数据。[2302] 履行数据保留职责是一种避免发生上述数据删除之前难于访问问题的方法。这种方法的一个具体实例是《欧盟数据保留指令》[2303]，2014 年该指令被宣布无效。[2304]

第 3 条——保留数据的义务

1. 按照欧盟文员会指令第 5、6、9 条中的克减条款，成员国应采取措施，保证按照此处的条款对该指令第 5 条规定的数据进行保留，前提是这些数据是在提供通信服务过程中，由公共电子通信服务或公共通信网络服务提供商在其权限范围内产生或处理的。

2. 第 1 段规定的数据保留义务应包括对第 5 条中指定的有关不成功呼叫请求数据的保留，这些数据是由公共电子通信服务或公共通信网络服务提供商在成员国管辖范围内产生、处理或存储（适用于电话数据）或记录（适用于互联网数据）的。本指令不应要求保留未连接呼叫的数据。

第 4 条——访问数据

各成员国应采取措施，确保符合本指令的数据保留应由特定领域的国家权威机构遵照国家法律来实施。为访问符合必要性和合理性要求的保留数据所遵循的程序以及需要满足的条件应在各成员国自己的国家法律中加以确定，同时要遵从欧盟法律或国际公法，特别是欧洲人权法院解释的 ECHR 中的有关条款。

第 5 条——需保留数据的类型

1. 各成员国应确保保留下列本指令规定的数据：

(a) 用于跟踪和确认通信源头的数据：

(1) 有关固定网络电话和移动电话的数据：

(i) 呼叫电话号码；

(ii) 普通用户或注册用户的姓名和地址；

(2) 有关互联网访问、网络电子邮件和国网络电话的数据：

(i) 为用户分配的 ID 号；

(ii) 接入公用电话网络任何通信服务的用户 ID 和电话号码；

(iii)普通用户或 IP 地址的注册用户的姓名和地址、通信过程中分配的用户 ID 或电话号码；

(b) 用于跟踪和确认通信目的地的数据：

(1) 有关固定网络电话和移动电话的数据：

(i) 拨叫的号码（呼叫的电话号码），以及如果涉及呼叫转接或呼叫转移等其他附加服务时的路由号码：

(ii) 普通用户或注册用户的姓名和地址；

(2) 有关网络电子邮件和网络电话的数据：

(i) 网络电话呼叫预定接收者的用户 ID 或电话号码；

(ii) 用户或注册用户的姓名、地址或通信预定接收者的用户 ID；

(c) 用于确定通信日期、时刻和持续时间的数据：

(1) 有关固定网络电话和移动电话、通信的日期以及开始和结束时间的数据；

(2) 有关互联网访问、网络电子邮件和国网络电话的数据：

(i) 登陆和退出网络电子邮件服务或网络接入服务的某个时区内的日期和时间以及 IP 地址（静态地址、动态地址或互联网服务提供商为通信分配的地址）以及用户或注册用户的用户 ID：

(ii) 登陆和退出网络电子邮件服务或网络电话服务的某个时区内的日期和时间；

(d) 用于识别通信类型的数据：

(1) 有关固定网络电话和移动电话的数据：所使用的电话服务；

(2) 有关网络电子邮件和网络电话的数据：所使用的互联网服务：

(e) 用于识别用户通信设备或设备用途的数据：

(1) 有关固定网络电话的信息：主叫和被叫电话号码；

(2) 有关移动电话的信息：

(i) 主叫和被叫电话号码；

(ii) 主叫用户的国际移动用户标识：

(iii) 主叫用户的国际移动设备标识：

(iv) 呼叫方的 IMSI；

(v) 被叫方的 IMEI；

(vi) 预付费匿名服务时，首次激活服务的日期和时间以及激活服务所处的位置标签（移动电话 ID）；

(3) 有关互联网接入、网络电子邮件和网络电话的数据：

(i) 拨号上网时的主叫号码；

(ii) 数字用户线（DSL）或其他通信发起人端点；

(f) 用于识别移动通信设备位置的数据：

(1) 通信开始时的位置标签（移动电话 ID）：

(2) 用于通过参照位置标签确定通信数据保持期间蜂窝电话地理位置的数据。

2 根据本指令，不能保留反映通信内容的数据。

第 6 条——保留的期限

各成员国应确保第 5 条所列的数据类型的保留期限不得少于 6 个月，但不得超过 2 年（从通信发起时起算）。

第 7 条——数据保护与数据安全

在不影响采用指令 95/46/EC 和指令 2002/58/EC 中的条款的情况下，根据本指令，各成员国应至少确保公用电子通信服务提供商后公共通信网络服务提供商遵循下列有关数据保留的数据安全原则：

(a) 所保留的数据应与网络中的数据拥有同样的质量，并得到同样的安全保护：

(b) 对数据应采取合适的技术或组织措施，防止数据受到偶然的或非法的破坏、意外丢失或更改、或未授权或非法存储、处理、访问或披露。

(c) 对数据应采取合适的技术或组织措施，确保数据只能被授权用户访问；

(d) 除那些被访问和保存的数据外，其他数据在保留期结束后应予以销毁。

第 8 条——保留数据的存储要求

根据本指令，各成员国应确保第 5 条所列的数据按照如下方式被存储：所保留的数据以及与这些数据有关的其他必要信息可以在授权用户的请求下无延迟的传输。

指令涵盖有关所有网络通信关键信息这一事实已经引起了人权组织的强烈批评。[2305] 这反而促使宪法法庭对指令及其实施办法进行修订。[2306] 另外，在西班牙音乐制作人与西班牙电信公司的案件 [2307] 中，欧洲法院总法律顾问朱利安·柯克特在她的结论中指出，数据保留职责是否可以在不违反基本权益的情况下实施是个问题。[2308] 实施这项规定的困难也已经在 2010 年的八国集会中也指出了实施这项规定的困难。[2309]

但是批评并不仅限于这个方面，为什么数据保留已经在应对网络犯罪方面变得效率低下的另一个原因是该责任可以被绕过。最早绕过数据保留责任的方法包括使用不同的、不需要注册的互联网终端或预付费移动电话数据服务 [2310] 以及使用在一些国家不限定数据保留职责的国家实行的匿名通信服务（至少一部分是）。[2311]

如果违法者使用了不同的公共终端后预付费电话数据服务（在这些终端上他们不需要登记由提供商存储的数据），那么数据保留职责只能将执法机构引向服务提供商，而非真正的违法者。[2312]

另外，违法者还可以通过使用匿名通信服务器绕过数据保留职责。[2313] 在这种情况下，执法机构也许能证明违法者使用了匿名通信服务器这一事实，但却没有获得匿名通信服务器所在国的流量数据，这样他们将无法证明违法者是否参与了犯罪准备。[2314]

由于很容易绕过该职责条款，在偶欧盟建立数据保留立法伴随着对这一过程需要辅助措施来确保条款有效性的担心。可能的辅助措施包括在使用网络服务前进行注册的义务 [2315] 或禁止使用匿名通信技术。[2316]

2014 年，欧洲法院最终宣布该指令无效。[2317]法院认为，该指令对个人隐私权和个人资料保护权等基本权利构成了各种严重干扰，且相关干扰未被限制在严格必要层面。自此，各成员国均不再受该指令的约束，不过，因该指令衍生且已执行的国家法律则不会自动失效。目前尚不能确定的是欧盟是否将提出并通过一项新指令。

6.5.6 搜索与查封

尽管实时收集内容数据进而使用远程取证软件确定违法者等新的调查方法正在讨论之中，并已在某些国家得到实施，但搜索和查封仍旧是最重要的调查方法之一。[2318] 一旦确定了违法者并且执法机构查封了其 IT 设备，计算机鉴定专家就可以对设备进行分析，来收集起诉所需要的证据。[2319]

当前在一些欧洲国家及美国正在讨论对搜索和查封程序进行更换和修改的可能性。[2320] 避免进入嫌疑人的住所来搜索和查封计算机设备的一种途径是利用在线搜索。这种方法将在后续的章节中进行详细的介绍，该方法规定了执法机构通过互联网进入嫌疑人的计算机进行秘密搜索的一种程序。[2321] 尽管执法机构可能得益于嫌疑人意识不到被调查的情况，但物理进入计算机硬件仍是一种更为有效的调查技术。[2322] 这一点更加突出了在互联网调查中搜索与查封的重要性。

欧洲理事会《网络犯罪公约》

大多数国家刑事诉讼法包含能使执法机构对特定对象进行搜索和查封的条款。[2323] 然而，为什么欧洲理事会《网络犯罪公约》的起草者将应对搜索和查封的条款包含其中的原因是国家法律通常不涉及与数据有关的搜索与查封程序。[2324] 例如，某些国家限制对查封对象使用查封程序。[2325] 根据这些条款，调查人员能够查封整个服务器，但不能仅通过将有关数据从服务器中复制出来的方式对其进行查封。在有关信息与成百上千其他用户的数据一同存储在服务器上，而这些数据在执法机构查封服务器后不再有用的情况下，使用这种方法存在一定的困难。针对可见项目的传统搜索和查封方法不够充分的一个具体实例是，执法机构不知道服务器的物理位置，但能够通过互联网进入该服务器。[2326] 与《网络犯罪公约》中的其他诉讼条款类似，第 19 条并不专门规定调查人员开展调查工作必须满足的条件和要求。该条款本身既没有说明法院判令的必要性，也没有说明在何种情形给出法院判令要求的例外情形。考虑到搜索与查封程序 [2327] 有可能侵犯嫌疑人的公民自由和权益的后果，大多数国家限制这种方法的适用性。[2328]

欧洲理事会《网络犯罪公约》第 19 条第 1 段旨在建立一种能够对计算机系统进行搜索的、与传统搜索程序同等有效的方法。[2329]

第 19 条——对已存储计算机数据的搜索与查封

1. 各方应采取必要的法律或其他措施，使其执法人员有权搜索或访问：
   a 计算机系统或部分计算机系统以及存储在该计算机系统中的计算机数据；
   b 计算机数据有可能存储其中的计算机数据存储介质。

[…]

尽管搜索与查封程序是调查人员经常使用的一种方法，但在将其应用于网络犯罪调查的过程中仍存在着很多困难。[2330] 主要的困难之一是搜索令通常限定于某些位置（如，嫌疑人的住所）。[2331] 搜索计算机数据的主要可能在于，在调查期间，嫌疑人并没有将数据存储在本地硬盘驱动器上，而是存储在可以通过互联网访问的外部服务器上。[2332] 使用互联网服务器存储数据和处理数据已经在互联网用户中逐渐普及（“云计算”）。在互联网服务器上存储信息的优点之一可以在任何有互联网连接的地点访问这些信息。为了确保能有效开展调查工作，在调查过程中保持一定的灵活性很重要。如果发现有关信息存储在另一计算机系统中，调查人员应能延伸搜索到该计算机系统。[2333] 欧洲理事会《网络犯罪公约》在其第 19 条第 2 段中解决了这一问题。

第 19 条——对已存储计算机数据的搜索与查封

[…]

2. 当其执法人员依照第 1 款 a 项对某一特定的计算机系统或部分计算机系统进行搜索或访问时，如果有理由相信所搜索的数据是存储在另一计算机系统或该系统的部分，而这些数据又可以通过本地系统进行合法访问，各方应采取必要的法律或其他措施，确保执法人员应能迅速延伸搜索或访问到另一计算机系统。

[…]

查封计算机数据存在另外一个问题。如果调查人员认为所查封的用于存储信息的硬件不是必要的或可能是不适当的，就需要有其他方法能继续实施对所存储的计算机数据的搜索和查封工作。[2334] 这类必要的方法不仅限于对有关数据的复制操作。[2335] 还有很多辅助措施对于维持所要求的效率是很有必要的，例如，对计算机系统本身的查封。[2336] 保持所复制数据完整性是一个最重要的方面。如果调查人员没有被允许采取必要的措施来保证所复制数据的完整性，那么，在刑事诉讼过程中，这样的数据有可能不会作为证据而被采纳。[2337] 调查人员复制了数据并采取了保持其完整性的必要措施，那就需要决定如何处理原始数据。因为在查封期间，调查人员不会移走硬件设备，所以，那些信息仍旧保存这些硬件设备上。尤其是在针对非法内容 [2338]（如，儿童色情资料）的调查过程中，调查人员不能将数据留在服务器上。因此，需要有一种方法能允许调查人员移走数据或至少确保这些数据不能再被访问。[2339] 欧洲理事会《网络犯罪公约》在其第 19 条第 3 段中解决了这一问题。

第 19 条——对已存储计算机数据的搜索与查封

[…]

3. 各方应采取必要的法律和其他措施，授权其主管部门查封或保护依照本条第 1 款或第 2 款所获得的计算机数据。这些措施应包括针对下列行为的授权：

a 查封或保护计算机系统或部分计算机系统或计算机数据存储介质；

b 制作、保留这些数据的一个备份；

c 保持有关已存储计算机数据的完整性；

d 禁止访问或移除这些计算机系统中的计算机数据。

[…]

与计算机数据搜索令有关的另一问题是，执法机构有时难以发现数据的位置。通常这些数据是存储在特定国领土范围之外的计算机系统中。即使已知其准确位置，但大量的数据却又成为快速调查的障碍。[2340] 在这些情况下，面临着非常特殊的困难就是调查工作是在国际范围内开展的，所以需要在调查过程中进行国际合作。[2341] 即使所调查的计算机系统位于国内，并且调查人员已经确定了运行违法者存储相关数据的服务器的主机提供商，调查工作还有可能面临确定数据准确位置的困

难。非常有可能出现的情况是，甚至中小规模的主机提供商也拥有数以百计的服务器和数以千计的硬盘。通常，调查人员在负责服务器基础设施的系统管理员的协助下也无法确定准确位置。[2342] 但是，即使调查人员能够确定特定硬盘驱动器，这些设备中的保护措施也会阻止其开展对有关数据的搜查工作。《网络犯罪公约》的起草者决定采取一种便于搜索和查封计算机数据的强制性措施来解决这一问题。第 19 条第 4 款授权调查人员强制系统管理员来为执法机构提供帮助。尽管遵从调查人员指令的责任仅限于酌情提供必要的信息和支持，但这种方也改变了搜索和查封程序的特征。在很多国家，搜索和查封指令只是强制受调查工作影响的人来接受这一过程——他们不需要主动支持调查工作。对于拥有调查人员所需的专门知识的人员，欧洲理事会《网络犯罪公约》的实施会从两个方面改变现有情形。一个方面的变化是，这些人需要向调查人员提供必要的信息。第二个方面的变化与其责任有关。向调查人员提供合理支持的责任使具有专门知识的人不受契约责任或监督人员的指令的制约。[2343]《网络犯罪公约》没有定义“合理”这一术语，但解释性报告指出：合理“可以包括向调查机构提供口令或其他安全措施”，但一般不涉及“提供口令或其他安全措施”，虽然这与“无理威胁无权搜索的其他用户或其他数据的私密性”的性质相符。[2344]

第 19 条——对已存储计算机数据的搜索与查封

[…]

4. 各方应采取必要的法律和其他措施，授权其主管部门责令任何具有运行计算机系统或用于保护计算机数据的安全措施专门知识的人员尽可能为其提供必要的信息，以便保证第 1 款和第 2 款中所涉及的措施的实施。

[…]

《英联邦计算机与计算机相关犯罪示范法》

2002 年的《英联邦示范法》给出了类似的方法。[2345]

此部分的定义

11 在这一部分中：

[…]

“查封”包括：

(a) 制作并保留计算机数据的备份，包括使用现场设备；

(b) 禁止访问或移除这些计算机系统中的计算机数据；

(c) 制作计算机数据输出的打印品；

[…]

搜索与查封 签发令

12[2346]**.** (1) 如果地方法官根据[誓词信息][宣誓]认定有合理的依据[怀疑][相信]某处的某物或某计算机数据：

(a) 可以作为重要的证据证明某一犯罪行为；或

(b) 已作为犯罪行为的后果被某人获取；

则地方法官[可以][应当]出具一份证明，授权[执法][警务]人员在必要的帮助下进入该处对该物或该计算机数据进行搜查。

[…]

协助警方

13[2347]

(1) 拥有或控制某依照第 12 节的规定进行搜查的计算机数据存储介质或计算机系统的人必须允许并协助搜查人员实施下列行为：

(a) 进入并使用计算机系统或计算机数据存储介质来搜查任何可用的计算机数据或计算机系统中的计算机数据；

(b) 获取并复制计算机数据；

(c) 使用设备制作备份；

(d) 从计算机系统中获得明文形式的、可理解的、可供人阅读的输出。

(2) 没有合法借口或理由拒不允许或协助搜查的人将被认定为实施了可处罚的犯罪行为，定罪时，可判处不超过[具体期限]的监禁，或处以不超过[具体数额]的罚金，或二者并罚。

6.5.7 制作订单

虽然欧洲理事会《网络犯罪公约》第 19 条第 4 段中的职责没有在国家法律中得以实施，服务提供商都会与执法机构合作，以避免对其业务造成负面影响。如果由于缺少服务提供商的合作而使调查人员无法找到他们所需要搜索和查封的数据或存储设备，那么调查人员就需要查封比实际需要更多的硬件设备。因此，服务提供商通常会支持调查工作，并在执法机构的要求下提供相关的数据。欧洲理事会《网络犯罪公约》包含允许调查人员在拥有相关数据的人员向调查人员提供了此类相关数据的情况下，无需搜查令而直接进行搜查的条款。[2348]

在没有法律依据的情况下，尽管执法机构和服务提供商的共同努力看起来是公私合作的一个很好的例子，但在不规范的合作下还存在很多困难。除了数据保护问题外，主要的问题在于如果服务提供商在没有充分法令律依据的条件下按照要求提供特定数据，这可能会违反其与客户之间的契约责任。[2349]

第 18 条——制作订单

1.各方应采取必要的法律和其他措施，使其主管部门有权要求：

a. 在其领土范围内的人提供其所拥有或控制的、存储在计算机系统或计算机数据存储介质中的特定计算机数据；

b. 在签约国领土范围内提供其服务的服务提供商提供其所拥有或控制的、与该服务有关的用户信息。

第 18 条包含两类责任。根据第 18 条第 1a 段，任何人（包括服务提供商）有责任提交其所拥有或控制的特定计算机数据。与第 1 款 b）项不同，该条款的应用并不限于特定的数据。术语“拥有”要求该人员能够物理进入到存储指定数据的数据存储设备。[2350] “控制”这一术语使本条款的应用范围得以扩展。数据是在某个人的控制之下，即使该人尚未物理进入存储设备，但能对信息进行管理。如果嫌疑人已经在远程存储系统中存储了有关的数据，那么这就是一个控制的例子。《网络犯罪公约》的解释性报告指出，单纯的远程访问存储数据的技术能力不一定构成控制。[2351]因此，欧洲理事会《网络犯罪公约》第 18 条的应用仅限于嫌疑人的控制程度超过了访问数据的潜在可能性的情形。

第 1b）分段包含一条鉴于特定数据的制作订单。根据第 18 条第 1 b) 分段，调查人员可以责令服务提供商提供用户信息。用户信息对于确定违法者是必要的。如果调查人员能够发现违法者所使用的 IP 地址，他们需要将这一地址对应到某个人。[2352] 在大多数情况下，IP 地址只会引向为用户提供 IP 地址的互联网服务提供商。在允许使用服务之前，互联网提供商同城要求用户用其用户信息进行注册。[2353] 第 18 条第 1 b）分段允许调查人员责令服务提供商提供其用户信息。在这种情况下有必要强调的是，欧洲理事会《网络犯罪公约》第 18 条既没有强加数据保留责任 [2354]，也没有服务提供商强加用户信息注册的责任。[2355]

第 1a) 分段中的“计算机数据” 与第 1 款 b)项中的“用户信息”之间的区别初看起来不是必然的，因此第 1a)分段也涉及以数字形式存储的用户信息。存在差异的第一个原因就是“计算机数据”和“用户信息”的定义不同。不同于“计算机数据”，术语“用户信息”不要求信息以计算机数据的形式存储。欧洲理事会《网络犯罪公约》第 18 条第 1b)分段使主管执法机构能够提供以非数字形式保存的信息。[2356]

第 1 条——定义

本公约下：

[...]

b “计算机数据”系指任何事实、信息或概念的表述，其形式为适合于在计算机系统中进行处理，计算机数据包括适合于让计算机系统完成特定功能的程序。

第 18 条——制作订单

[...]

3 在本条中，术语“用户信息”系指包含在计算机数据或服务提供商所拥有的其他（除流量或内容数据之外）的数据中且与其服务用户有关的信息，以及该信息赖以存在的下列信息：

a 所使用的通信服务的类型、所采取的技术以及服务的期限；

b 用户的身份信息、邮政或地理地址、电话和其他访问号码、服务协议或约定下的账单和付款信息；

c 在服务协议或约定下安装通信设备现场的其他任何信息。

区分“计算机数据”与“用户信息”的第二个原因是，它能使法律制定者对应用该条款提出不同的要求。[2357] 这有可能对第 1 款 b)项下的制作订单提出更为严格的要求，[2358] 因为本条款允许执法机构访问任何形式的计算机数据，包括内容数据。[2359] 实时收集流量数据（第 20 条）[2360] 与实时收集内容数据（第 21 条）[2361] 的区别表明，《网络犯罪公约》的起草者认识到需要实施不同的安全保障措施，这种不同取决于执法机构所访问的数据类型的不同。[2362] 由于“计算机数据”和“用户信息”之间存在着差异，所以欧洲理事会《网络犯罪公约》第 18 条允许签约国针对制作订单开发类似的分级保障系统。[2363]

《英联邦计算机与计算机相关犯罪示范法》

2002 年的《英联邦示范法》给出了类似的方法。[2364]

数据制作

15 在警察提出申请的基础上，如果地方法官认为指定的计算机数据、数据的打印输出或其他信息是出于犯罪调查或刑事诉讼的目的而被合理使用，该地方法官可以要求：

(a)[颁布国]领土范围内控制计算机系统的人从其计算机系统中产生出指定的计算机数据、数据的打印输出或该数据的其他可理解的输出；

(b) [颁布国]领土范围内的互联网服务提供商准备有关订购或使用其服务的人的信息；

(c)[2365] [颁布国]领土范围内已进入指定计算机系统的人在其计算机系统中处理、编辑指定的计算机数据并将这些数据提供给指定的人。

6.5.8 数据的实时收集

电话监听是一种很多国家在死刑犯罪调查过程中使用的方法。[2366] 很多犯罪分子在犯罪准备和实施犯罪过程中都会使用电话，特别是移动电话。尤其是在毒品非法交易案件中，监听罪犯之间的对话对调查工作的成功可能是必不可少的。该条款允许调查人员收集有用的信息，尽管这些信息仅限于通过所监控的线路/电话交换的信息。如果犯罪分子采用其他信息交换形式（如，信件）或使用不在监控范围内的线路进行信息交换，调查人员将不能记录对话信息。一般来说，当不使用电话进行信息交换时，情况是相同的。[2367]

如今，数据交换已经取代了传统的电话通话。数据交换不限于电子邮件或文件传输。使用基于 IP 协议的技术开展的话音通信（网络电话）的数量逐渐增加。[2368] 从技术的角度看，网络电话呼叫进行信息交换完全超过了使用电话线的传统电话呼叫。截获这类呼叫困难极大。[2369]

由于很多计算机犯罪都涉及数据交换，因此截获这类交换过程或使用与交换过程有关的数据的能力对于成功的调查过程是必不可少的要求。现有电话监听条款以及有关在网络犯罪调查过程中使用电信流量数据的条款的应用在有些国家已经变得很困难。所面临的困难既是技术问题 [2370] 也是法律问题。从法律角度看，授权记录电话信息不一定包括授权监听数据传输过程。

欧洲理事会《网络犯罪公约》旨在填补执法机构在监控数据传输过程的能力方面的空缺。[2371] 在这一方法中，《网络犯罪公约》在数据传输监控的两个子集之间进行了区分。第 20 条授权调查人员收集流量数据。术语“流量数据”在《公约》的第 1 条 d)段中进行了定义。

第 1 条——定义

[...]

d. “流量数据”系指任何通过计算机系统通信有关的计算机数据，该数据由构成通信链路一部分的计算机系统产生，能够表明通信的信源、信宿、路径、时间、数据、大小、持续时间或服务类型。

“内容数据”和“流量数据”的区别与大多数相关国家法律之间的区别相同。[2372]

6.5.9 流量数据的收集

欧洲理事会《网络犯罪公约》

考虑到国与国之间对流量数据的定义各不相同，[2373] 欧洲理事会《网络犯罪公约》的起草者决定对这一术语进行定义，以便改善有关条款在国际调查中的应用条件。“流量数据”这一术语用于描述通信过程中由计算机产生的数据，以便找出信源到信宿之间的通信路径。每当用户连接到互联网，下载电子邮件或打开某个网站时，就会产生流量数据。对于网络犯罪调查，关系最为密切的是能够确定基于互联网的通信各方身份的信源和信宿的 IP 地址。[2374]

不同于“内容数据”，“流量数据”这一术语只涉及数据传输过程中产生的数据，而非所传输的数据本身。尽管在某些情况下，为了执法机构能更有效地对通信进行分析可能有必要获取内容数据，但在网络犯罪调查过程中，“流量数据”的重要性更加突出。[2375] 虽然获取内容数据能够使执法机构对所交换的消息或文件的特点进行分析，但流量数据对于确定违法者可能是必要的。例如，在儿童色情资料案件中，流量数据能够使调查人员确定违法者正在下载儿童色情图像的网页。通过监测使用互联网期间产生的流量数据，执法机构能够确定服务器的 IP 地址，而后可以进一步确定其物理位置。

第 20 条——实时收集流量数据

1. 各方应采取必要的法律和其他措施，授权其主管部门实施下列行为：
   a 在签约方的领土范围内利用技术手段实时收集或记录，并且
   b 强制服务提供商在其现有技术能力条件下：
      i 在签约方的领土范围内利用技术手段实时收集或记录，或
      ii 与主管部门合作或协助主管部门实时收集或记录利用计算机系统在其领土范围内进行的特定通信的流量数据。
2 如果签约方由于其国内法律体系中现有的法律原则而不能使用第 1 款 a 项的规定，可以采用必要的替代法律和其他措施，确保在其领土范围内通过技术手段所进行通信的流量数据的实时收集或记录。
3 各方应采取必要的法律和其他措施，责成服务提供商保持履行本条赋予的权力和任何与之有关的信息的机密性。
4 本条所涉及的权力和程序应当遵从第 14 条和第 15 条的规定。

第 20 条包含两种收集流量数据的不同方法，任何一种方法都有可能被采纳。[2376]

第一种方法是对互联网服务提供商强加一种能使执法机构直接收集相关数据的责任。这通常需要安装执法机构用于访问互联网服务提供商基础设施的接口设备。[2377]

第二种方法是执法机构能够强令互联网服务提供商按其要求收集数据。这种方法使调查人员能利用服务提供商的现有技术能力和知识。将两种方法合二为一的一个目的是确保在服务提供商没有合适的技术来记录数据的情况下，执法机构应能在没有提供商协助的情况下（依照第 20 条第 1 b）分段开展调查工作。[2378]

起草欧洲理事会《网络犯罪公约》既不倾向于专门的技术，也不倾向于为行业建立需要很高金融投资的标准。[2379] 从这一观点看，《网络犯罪公约》第 20 条第 1 款 a)项也许是较好的解决方案。然而，第 20 条第 2 段中的规定说明了《网络犯罪公约》的起草者意识到有些国家在实施允许执法机构直接开展调查工作的立法时存在一定的困难。

根据第 20 条开展调查工作的主要困难之一是匿名通信技术的使用。正如以上所解释，[2380] 犯罪分子可以利用互联网服务实施匿名通信。如果犯罪分子正在使用“突岩”软件之类的匿名通信服务，[2381] 在大多数情况下，调查人员无法分析流量数据，也无法成功确定通信双方。犯罪分子可以通过使用公共互联网终端来达到统一的效果。[2382]

与传统搜索与查封程序相比，收集流量数据的一个优点在于犯罪嫌疑人不一定意识到正在开展的调查工作。[2383] 这就限制了嫌疑人销毁证据的可能性。为了确保服务提供商没有将有关正在进行的调查工作告知犯罪分子，第 20 条第 3 段解决了这一问题，并责成签约国实施立法，确保服务提供商保守现有调查工作的机密性。对于服务提供商而言，其好处在于能使提供商免除通知用户的义务[2384]。[2385]

欧洲理事会《网络犯罪公约》设计用来改善和协调有关网络犯罪问题的立法。[2386] 在这种情况下有必要强调的是，第 21 条中的条款不仅适用于关于网络犯罪的犯罪行为，也适用于任何犯罪行为。如果使用电子通信不仅在网络犯罪案件中有显著的作用，而且在网络犯罪之外应用本条款进行调查的过程中也很有用。这有可能使执法机构能使用那些准备实施传统犯罪的犯罪分子之间进行电子邮件交换过程中产生的流量数据。第 14 条第 3 段赋予各签约方权力，使其能对本条款在特定犯罪行为中的应用做出保留和限制。[2387]

《英联邦计算机与计算机相关犯罪示范法》

2002 年的《英联邦示范法》给出了类似的方法。[2388]

流量数据的截获

19. (1) 如果警察认定与特定通信有关的流量数据是出于犯罪调查的目的而被合理使用，他可以通过书面通知控制这类数据的人的形式要求该人：

(a) 收集或记录与特定通信有关的、规定期限内的流量数据；

(b) 允许并协助警察收集或记录该数据。

(2) 如果地方法官根据[宣誓信息][誓词] 有合理的理由[认定]流量数据是出于犯罪调查的目的而被使用，他[可以][应当]授权警察收集或记录与特定通信有关的、规定期限内通过使用技术手段产生的流量数据。

6.5.10 内容数据的截获

欧洲理事会《网络犯罪公约》

第 21 条除了在处理内容数据方面与第 20 条类似外，其结构也与第 20 条类似。在执法机构已经知道通信双方的身份但被有信息交换的类型的情况下，能够监听数据交换过程对于是很重要的。第 21 条为执法机构记录数据通信和分析内容提供了可能。[2389] 这些信息包括从网站或文件共享系统上下载的文件、违法者发送或接收的电子邮件以及聊天记录。

第 21 条——内容数据的截获

1 在国内法律认定为严重犯罪的范围内，各方应采取必要的法律和其他措施，授权其主管部门实施下列行为：

a 在签约方的领土范围内利用技术手段实时收集或记录，并且

b 强制服务提供商在其现有技术能力条件下：

i 在签约方的领土范围内利用技术手段实时收集或记录，或

ii 与主管部门合作或协助主管部门实时收集或记录利用计算机系统在其领土范围内进行的特定通信的内容数据。

2 如果签约方由于其国内法律体系中现有的法律原则而不能使用第 1 款 a 项的规定，可以采用必要的替代法律和其他措施，确保在其领土范围内通过技术手段所进行通信的内容数据的实时收集或记录。

3 各方应采取必要的法律和其他措施，责成服务提供商保持履行本条赋予的权力和任何与之有关的信息的机密性。

4 本条所涉及的权力和程序应当遵从第 14 条和第 15 条的规定。

不同于流量数据，欧洲理事会《网络犯罪公约》并没有给出内容数据的定义。真如其本身的含义，“内容数据”这一术语指的是通信的内容。

网络犯罪调查中的内容数据的具体实例包括：

- 邮件主题；
- 嫌疑人打开的网站上的内容；
- 网络电话的谈话内容。

依照第 2 条进行调查的最大的困难是以是机密技术的使用。[2390] 正如之前所详述，使用加密技术可以使违法者将内容改变为执法机构无法访问的形式。如果违法者对其所传输的内容进行加密，执法机构只能截获加密了的通信数据，却无法对齐内容进行分析。如果没有加密所使用的密钥，任何可能的解密操作可能要花费很长时间。[2391]

《英联邦计算机与计算机相关犯罪示范法》

2002 年的《英联邦示范法》给出了类似的方法。[2392]

电子通信的截获

18. (1) 如果[地方法官][法官]根据[宣誓信息][誓词]认定有合理的理由[怀疑][相信]电子通信的内容是出于犯罪调查的目的而被使用的，该地方法官[可以][应该]：

(a) 要求在[签约国]提供服务的互联网服务提供商利用技术手段收集或记录、或允许或协助主管部门收集或记录利用计算机系统实施的特定通信传输中的内容数据；或

(b) 授权警察利用技术手段收集或记录数据。

6.5.11 与加密技术有关的规定

如上所述，犯罪分子还可以通过加密技术妨碍内容数据的分析。可供使用的各种软件产品能够使用户有效地保护文件和数据传输过程，使其免受未授权访问。[2393] 如果嫌疑人已经使用了这类产品，而调查机构没有得到加密文件所用的密钥，那么所需要的解密过程可能需要很长时间。[2394]

犯罪分子使用加密技术对于执法机构而言是一个挑战。[2395] 现在有很过国家和国际方法 [2396] 来解决这一问题。[2397] 由于对加密技术有着不同的评价，目前还没有广泛公认的国际方法来解决这一问题。

一种方法是授权执法机构在必要时破译密码。[2398] 如果没有授权或没有发出制作订单的可能性，执法机构就无法收集必要的证据。另外，或作为一种选择，可以授权调查人员使用键盘记录软件来截获加密文件的密码，以便破译改密码。[2399]

另一种方法是通过限制密钥长度的方法来限制使用加密软件。[2400] 根据限制的程度，这有可能使调查人员在合理的时间期限内破译密码。这一解决方法的反对者担心这种限制不仅有可能使调查人员破译密码，还有可能使经济间谍尝试获取加密了的商业信息。[2401] 另外，如果可以使用这种该软件工具，那么这种限制有可能仅仅限制了犯罪分子使用更强大的密码。这有可能首先要求有国际标准来防止强密码产品的制造者在其国内提供未加任何适当密钥长度限制的产品。在任何情况下，犯罪分子可能会开发自己的、没有任何密钥长度限制的加密软件。

另一种方法是强制为强密码产品建立密钥托管制度或密钥恢复程序。[2402] 执行这样的规定可能会使用户继续使用强密码技术，但也能使调查人员通过强令用户将密钥提交给保存密钥并在必要时将密钥提供给调查人员的专门机构的方式获取有关的数据。[2403] 这种方法的反对者担心有人会得到提交的密钥，并用这些密钥来解密秘密信息。另外，犯罪分子有可能通过开发无需向有关部门提交密钥的加密软件的方式轻易绕过这些规定。

最后，各国试图通过执行制作订单的方式来解决这一问题。[2404] “制作订单”这一术语规定了披露加密数据所用密钥的义务。1997 年在丹佛举行的八国集团会议对这一条款的实施进行了讨论。[2405] 很多国家已经落实了该义务。[2406] 印度《信息技术法》第 69 节的规定就是落实该义务的一个具体实例。[2407] 2000 年的英国《调查权力规范法》第 49 节给出了落实该义务的另一个实例：[2408]

要求披露的通知

49.

(1) 本节内容适用于下列情形：

(a) 受保护的信息已经为任何人通过履行法定的查封权、扣留权、检查权、搜查权或文件或财产干涉权，或类似的手段所拥有；

(b) 受保护的信息已经为任何人通过履行法定权力监听通信，或类似的手段所拥有；

(c) 受保护的信息已经为任何人通过履行任何第 22 节第 3 款或第 II 部分赋予的权力、或根据第 22 节第 4 款通知履行权力或类似的手段所拥有；

(d) 受保护的信息已经为任何人因依照任何法定义务供给或披露（不论结果是否是由对信息的请求而产生）或类似的手段所拥有；

(e) 受保护的信息已经为任何情报机构、警察或海关和税务局利用除法定权力之外的任何其他合法手段所拥有，或类似的手段为这些机构、警察或海关和税务局所拥有。

(2) 如果拥有符合第 2 款要求的适当许可权任何人有合理的根据相信：

(a) 保护信息的密钥为任何人所拥有，

(b) 对受保护信息的强制披露要求（i） 符合第 3 小节的要求或（ii）是出于确保任何拥有任何法定权力或法定义务的公共机关有效履行职责或采取合理的措施，

(c) 强制披露要求符合其预定的目标，

(d) 拥有适当许可权的人在没有得到本节所规定的许可的情况下，以可理解的形式获得受保护的信息是相当不合理的，拥有该许可权的人可以通过告知其确认为掌握密钥的人，强迫该人披露受保护的信息。

(3) 如果披露任何受保护信息的要求是出于以下目的，则该要求应符合本小节的规定：

(a) 符合国家安全的利益；

(b) 为了防止或消除犯罪；或

(c) 出于英国经济福利的利益。

(4) 本节所涉及的披露任何受保护信息要求的通知：

(a) 必须书面下达，或（如果没有书面下达）必须以留存记录的形式下达；

(b) 必须描述与通知有关的受保护信息；

(c) 必须指明符合第 2 小节 b 款第(i)项 或第 (ii)项要求的事项的通知对象；

(d) 必须指明下达通知者的官职、等级或职务；

(e) 必须指明符合第 2 条的授权下达通知者的官职、等级或职务，或（如果下达通知者有权在没有其他人许可的情况下下达通知）必须指明所获权利的背景；

(f) 必须指明通知起草的时间；

(g) 必须通知所要求的信息披露情况以及通知下达的形和方式，以及（f）款所规定的时间必须在所有情况下在一定时期内都符合要求。

为了确保要求公开密钥的人遵从指令并且真正提交了密钥，2000 年的英国《调查许可权规范法案》包含一条对不遵从指令定罪的条款。

不遵从通知。

53

(1) 如果某个已收到第 49 节所述通知的人故意不按照通知要求披露所要求的信息，则判定其有罪。

(2) 在针对任何本节认定为犯罪之人的诉讼案件中，如果已经证明该人在收到第 49 节所涉及的通知之前已经拥有任何受保护信息的密钥，则该人应出于此次诉讼案件的目的继续在随后的时间内拥有该密钥，除非已经证明，该密钥从下达通知之后到要求公开密钥的时刻这一时期内已不再拥有该密钥。

(3) 出于本节的目的，如果满足下列条件，则应证明该人在特定的时间未拥有受保护信息的密钥：

(a) 所列举的该事实的证据对拥有密钥提出质疑；

(b) 没有证明相反的情况超出合理怀疑的范围。

(4) 在针对任何本节认定为犯罪之人的诉讼案件中，如果涉案人能提供下列信息，则可以认定为辩护：

(a) 在收到第 49 节所述通知时，按照该通知的要求在通知规定时间之前进行披露对涉案人不是合理可行的；但

(b) 涉案人在上述合理可行的时间到来后立即进行披露。

(5) 犯有本节下规定的犯罪行为应当受到如下刑罚：
(a) 在指控定罪时，可以判处 2 年以下有期徒刑或罚金，或而这并罚；
(b) 在即决定罪时，可以判处 6 个月以下有期徒刑或处以不超过法定数额上限的罚金，或二者并罚。

[…]

2000 年的英国《调查许可权规范法案》要求犯罪嫌疑人具有支持执法机关工作的义务。[2409]

与此规则相关的一项一般性关切是，这种义务有可能与嫌疑人在自证犯罪方面的基本权益发生冲突。[2410] 嫌疑人需积极支持调查工作，而不是由主管部门单独完成调查工作。很多国家防止自证犯罪的强有力措施所产生的问题是，这样的防护措施何时才能变为一种示范性的解决方案，用以解决加密技术带来的问题。[2411]

另一个要考虑的问题是丢失密钥有可能导致刑事调查。尽管刑事定罪要求嫌疑人犯罪分子故意拒绝公开密钥，丢失密钥可能会使使用密钥的人卷入不必要的刑事诉讼中。但是，第 53（2）节的规定有可能干涉举证责任。[2412]

最后一个要考虑的问题是，技术方案能使嫌疑人免除公开加密所使用密钥的义务。嫌疑人如何免除透露密钥义务的一个实例是根据“合理推诿”[2413]原则使用加密软件。[2414]

6.5.12 远程取证软件

如以上所解释，在嫌疑人的计算机上寻找证据要求物理进入相关的硬件（计算机系统和外部存储介质）。这一程序通常意味着需要进入嫌疑人的公寓、住所或办公室。在这种情况下，只要调查人员开始着手进行搜索，嫌疑人就会意识到正在开展的调查工作。[2415] 这一信息可能会导致行为上的改变。[2416] 例如，如果嫌疑人攻击某些计算机系统，已测试其能力，从而为将来某一天与其他犯罪分子发起大规模攻击做准备，那么搜索程序就有可能妨碍调查人员确定其他嫌疑人，因为嫌疑人有可能停止与其他嫌疑人之间的联系。

为了避免所进行的调查工作不被发现，执法机构需要能使其接触到存储在嫌疑人计算机上的计算机数据、并能像电话呼叫监控一样被秘密使用的相关法律条款。[2417] 这样的法律条款可能会使执法机构远程进入嫌疑人的计算机系统来搜索信息。目前，正在集中讨论这类法律条款的必要性。[2418] 早在 2001 年就已经有报告指出美国联邦调查局正在为互联网有关的调查工作开发一种名为“幻灯”的键盘记录器。[2419] 2007 年就有报告指出，美国的执法机构正在使用软件来追踪使用匿名通信手段的嫌疑人。[2420] 该报告提及当需要使用一个名为 CIPAV [2421] 的工具时所需要的搜查令。[2422]德国联邦法院决定现有刑事诉讼法条款不再允许使用远程取证软件来搜查嫌疑人的计算机后，有关是否需要对这个领域现有的法律进行修订的争论就开始了。[2423] 在争论过程中所透露出来的信息是调查机构已经在很多调查工作中非法使用了远程取证软件。[2424]

“远程取证软件”的不同概念，特别是其所具有的功能已经在讨论中。[2425] 理论上看，软件应具有下列功能：其中之一可能就是搜索功能。这一功能使执法机构能搜查非法内容，并收集有关存储在计算机中的文件的信息。[2426] 另一种可能的功能是记录功能。调查人员能够记录嫌疑人计算机系统中没有永久存储的数据。例如，如果嫌疑人使用网络电话服务与其他嫌疑人联系，通常可能不会存储通话内容。[2427]远程取证软件可以记录经过处理的数据并为调查人员保存这些数据。如果远

程取证软件包含记录键盘敲击的模块，该模块可以用来记录嫌疑人用来加密文件所用的口令。[2428] 此外，这样的工具可能包括鉴别功能，这样，即使嫌疑人使用匿名通信服务使调查人员难以通过回溯追踪所使用的 IP 地址的方式确定犯罪分子，也能使调查人员证实嫌疑人参与到犯罪行为中。[2429] 最终，远程软件可能会出于住所监控的目的被用作启动网络摄像头或麦克风的工具。[2430]

尽管远程取证软件的这些功能看起来对调查人员非常有用，但有必要指出的是，使用这些软件在法律和技术方面还存在很多困难。从技术角度看，需要考虑一下几个方面的问题：

安装过程中的困难

远程取证软件需要被安装在嫌疑人的计算机上。恶意软件的传播证明，不经允许在互联网用户的计算机上安装软件是有可能的。但病毒和远程取证软件的区别在于，远程取证软件需要被安装在特定的计算机（嫌疑人的计算机）上，而计算机病毒的目的在于尽可能影响到更多的计算机，而无需集中于特定的计算机系统。有很多技术能使软件被传送到嫌疑人的计算机中。具体的方法有：通过物理进入的方式进行安装、将软件放在网站上供下载、在线访问计算机系统以避开安全措施以及将软件以难以察觉的形式隐藏在互联网运行期间出生的数据流中。[2431]由于大多数计算机都有病毒扫描器和防火墙之类的保护措施，所有的远程方法对调查人员来说都是很可能的。[2432]

物理进入的优点

开展的各种分析（如数据处理介质的物理检查）都需要进入硬件设备。而远程取证软件可能只能让调查人员对连接到互联网的计算机系统进行分析。[2433]此外，远程开展取证工作很难保证嫌疑人计算机系统的完整性。[2434] 在这方面，远程取证软件一般不可能代替对嫌疑人计算机进行的物理检查。

另外，在实施能使调查人员安装远程取证软件的法律条款之前，还需要考虑很多法律方面的问题。很多国家的刑事诉讼法和宪法中规定的安全保障措施限制使用这种软件的部分功能。在国家层面上，安装远程取证软件可能违反国家主权原则。[2435] 如果软件被安装在一台带出国境的笔记本电脑中，该软件可能使调查人员未经主管部门的允许在国外开展犯罪调查工作。

实例

由 HIPCAR 发起国中的受益国制定的立法文本中有一种此类方法的实例。[2436]

取证软件

27 (1) 在对此后第 5 款所列的犯罪行为进行调查时，如果（地方）法官根据[宣誓信息/誓词]有合理的理由相信，利用列于第四部分的其他法律条款无法收集到关键证据，但这些证据又是出于犯罪调查的目的而被合理要求的，那么，[法官/地方法官][可/须] 根据警察的申请使用带有调查所需的特殊任务的远程取证软件，并将其安装在嫌疑人的计算机上，用来收集相关证据。该申请应包含以下信息：

(a) 犯罪嫌疑人，如有可能的话，还应包括嫌疑人的姓名和地址，

(b) 目标计算机的描述，

(c) 准备使用的措施、范围和使用期限，

(d) 应用必要性的理由。

(2) 在这类调查过程中，有必要确保对嫌疑人计算机系统的修改仅局限于那些调查工作所需要的计算机系统，如有可能，任何改变都应该在调查结束后及时恢复。在调查期间，有必要记录下列信息：

(a) 所使用的技术手段以及实施的时间和日期；

(b) 计算机系统的标识和调查期间所做的修改；

(c) 获取的任何信息。

使用这类软件所获得的所有信息需要进行保护，防止其被修改、未授权删除和未授权访问。

(3) 第 27 节第 1 款授权的期限为[3 个月]。如果不再满足授权的条件，应立即停止行动。

(4) 安装软件的授权包括远程访问到嫌疑人的计算机系统。

(5) 如果安装过程需要物理进入某处，需要符合第 20 节的要求。

(6) 如有必要，警察[警官]可以依照第（1）款中的法院判令要求法院[执法]，责成互联网服务提供商来支持安装过程。

(7) [犯罪行为列表]

(8) 各国可以决定是否采用第 27 节。

立法文本的起草者指出，他们已经意识到使用该条款可能会严重干扰何人干涉嫌疑人的基本权益。[2437]因此，已经有多种安全保障措施得以实施。首先，使用软件要求不能通过其他途径收集证据，其次，需要法官或地方法官的判令。第三，应用该条款需要保证四个关键要素。除此之外，授权行为只能通过第 1 条和第 2 条加以限定。

6.5.13 授权要求

犯罪分子可以采取一定的手段是调查工作复杂化。除了使用匿名通信软件外，[2438]如果嫌疑人使用公共互联网终端或打开无线网络，鉴别工作就会变得很复杂。限制制作能使用户隐藏其身份信息并使公共互联网访问终端可用而无需身份认证的软件可以帮助执法机构更有效地开展调查工作。《意大利法令 144》[2439]第 7 条[2440]是限制使用公共终端来实施犯罪行为的方法的一个实例，该法令 2005 年升级成为法律（法律编号：155/2005）[2441]。该条款强制有意提供公共互联网访问服务（如网吧或网上大学[2442]）的任何人申请授权。除此之外，所涉及的人员被责令从其客户获得身份证明。由于建立无线接入点的个人通常不承担这种义务，所以，如果犯罪分子使用为首保护的专用网络来隐藏其身份，就可以轻易躲过监控。[2443]

调查工作的进展程度是否能证明对访问互联网和匿名通信服务的限制是个问题。目前，自由访问互联网已经是自由获取信息的一个重要方面，在很多国家受宪法的保护。如 2005 年的《联合国意见与表达自由特殊报告员、OSCE 媒体自由代表和 OAS 自由表达特殊报告员联合声明》强调，限制义务可以阻止未授权运行网络服务。[2444]要求进行身份认证可能会影响互联网的使用，因为用户在使用互联网时担心其行为被监控。即使用户知道他们的行为是合法的，身份认证这样的做法仍会影响用户间的相互交流。[2445]同时，试图免于身份认证的犯罪分子可以轻易躲过身份认证程序。例如，他们能使用在国外购买的无需身份认证的预付费电话卡访问互联网。

在针对匿名通信服务的立法也存在类似的问题。当前争论的焦点是，所讨论的关于加密技术的类似条款是否适用于匿名通信技术和服务。[2446]除了保护私密性和保障调查犯罪能力之间存在的冲突外，解决加密问题的各种法律方法（尤其是缺少可知行性的方法）同样适用于匿名通信的可行性也在讨论之中。

6.6 国际合作

参考书目（节选）： *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4; *Choo,* Trends in Organized Crime, 2008, page 273 *et seq.*; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005; *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1; *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992; *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2; *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296; *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931; *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9; *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

6.6.1 引言

日益增长的网络犯罪具有国际维度。[2447] 正如前文所述，隐藏在此现象背后的原因之一，就是犯罪分子几乎不需亲临服务提供现场这一事实。[2448]因此，罪犯通常无需出现在受害人所在位置。由于迄今为止尚未建立一综合性国际法律框架，也没有一超国家的实体能够调查此类犯罪，所以跨国犯罪需要相关各国有关机构之间的合作。[2449] 罪犯的流动性以及罪犯是否在场与犯罪结果之间的无关性，必然就需要执法和机构司法机构与拥有假定管辖权的国家之间的合作与协助。[2450] 由于各国法律与限制措施之间的差异性，国际合作始终被认为是应对犯罪全球化的主要挑战之一。[2451] 这与跨国犯罪以及网络犯罪的传统形式是直接相关的。调查人员在跨国调查中最主要需求之一，就是要求罪犯所在国家的相应机构作出即时的反应。[2452] 特别的，在涉及此类问题时，刑法事务中国际司法合作的传统措施手段，往往无法满足互联网犯罪调查在速度方面的要求。[2453]

6.6.2 国际合作机制

对于网络犯罪调查，用于支持国际合作的最为正式的机制就是司法协助和引渡。其他诸如刑事司法中罪犯移交、案件移交、没收犯罪所得以及资产回收等机制，在实践中往往并不是那么重要。除上述的正式机制外，还有不同国家法律执行机构间的情报交换等非正式手段。

6.6.3 可适用措施总览

当涉及国际合作可适用措施的辨识时，主要有 3 种情况可供考察。第一种情况是，其相关程序性措施可能是国际性协议（例如《联合国打击跨国有组织犯罪公约》（UNTOC）[2454] 及其 3 个附加协议[2455]）或区域协定（例如《美洲国家之间的刑事司法协助公约》[2456]、《欧洲刑事司法协助公约》[2457] 以及欧洲理事会《网络犯罪公约》）的构成部分 [2458]。第二种可能性是受到双边协议规管的程序性措施。此类协议通常会涉及应予提交的特殊请求、具体联络程序与联络形式的定义，以及请求国和被请求国之间的权利和义务等。[2459] 例如，澳大利亚与其他国家就引渡问题签署了超过 30 个双边协议。[2460] 此类协议的一些谈判可能也会将打击网络犯罪作为其主题之一，但是就现有协议对网络犯罪应管辖到何种程度仍具有不确定性。[2461] 如果既没有多边协议也没有双边协议可供适用，那么国际合作通常就需要建立在基于互惠原则的国际礼节的基础之上。[2462] 由于建立在双边协议和国际礼节基础之上的合作严重依赖于具体案件的实际情况以及相关各国，所以下文评述的重点将集中于国际性公约和区域性公约。

6.6.4 联合国《打击跨国有组织犯罪公约》

在刑事司法领域，司法合作的主要国际性措施就是联合国《打击跨国有组织犯罪公约》（UNTOC）。[2463] 此公约中包含有国际合作的重要措施，但其并不是专门用于解决网络犯罪的相关问题，也未就如何处理数据保护的紧急请求作出明确的规定。

联合国《打击跨国有组织犯罪公约》的适用范围

依照《公约》第 3 条第 1 段之规定，此公约仅适用于那些涉及有组织犯罪集团的网络犯罪案件。UNTOC 公约第 2 条中将“有组织犯罪集团”定义为由三人或多人所组成的，有组织结构的犯罪集团。

> **第 2 条.** 术语的使用
>
> 在本公约中：
>
> (a) “有组织犯罪集团”系指由三人或多人所组成的、在一定时期内存在的、为了实施一项或多项严重犯罪或根据本公约确立的犯罪以直接或间接获得金钱或其他物质利益而一致行动的有组织结构的集团；
>
> [...]
>
> **第 3 条.** 适用范围
>
> 1. 本公约除非另有规定，应适用于对下述跨国的且涉及有组织犯罪集团的犯罪的预防、侦查和起诉：
>
> (a) 依照本公约第 5 条、第 6 条、第 8 条和第 23 条确立的犯罪；
>
> (b) 本公约第 2 条所界定的严重犯罪。

因此，此公约特别规定适用于包含有组织犯罪形式的案件。毫无疑问，有组织犯罪中包含网络犯罪。但是，就跨国网络犯罪调查而言，UNTOC 公约对其的包含程度以及二者之间的相关性都是不明确的。作为一个事实上的问题，确定是否涉及有组织犯罪与公约的可适用性是高度相关的。但是，分析与身份有关犯罪与有组织犯罪之间的联系目前尚有困难。其中最主要的障碍就是在此领域内缺乏可信的科学研究。与犯罪的技术特征分析不同，对犯罪行为中的有组织犯罪成分还缺乏深入的分析。虽然已通过成功的调查确认过一些涉及网络犯罪的犯罪团伙，但是这些犯罪集团的组织结构，与跨国有组织犯罪集团的组织结构相比未必具有可比性。网络犯罪集团的组织结构往往更为松散，同时也更加灵活。[2464] 此外，网络犯罪集团的规模通常也会远远小于传统的有组织犯罪集

团。[2465] 互联网使人们能够与其他人密切合作，根本无需面对面相遇即进行行动的协调。[2466] 这也使得罪犯以不固定的特别团伙的形式实施共同犯罪成为可能。[2467].

有关相互司法协助的请求

有关相互司法协助的程序定义于《公约》第 18 条。本条款中规定了一套完整的程序。

> **第 18 条.** 相互司法协助
> 1. 缔约国应在对本公约第 3 条规定所涵盖之犯罪行为进行的侦查、起诉和审判程序中相互提供最大程度的司法协助；在请求缔约国有合理理由怀疑第 3 条第 1 款(a)项或(b)项所述之犯罪具有跨国性质时，包括怀疑此类犯罪的被害人、证人、犯罪所得、工具或证据位于被请求缔约国，而且该项犯罪涉及一有组织犯罪集团时，还应对等地相互给予类似协助。
> 2. 对于请求缔约国根据本公约第 10 条可能追究法人责任的犯罪所进行的侦查、起诉和审判程序，应当根据被请求缔约国有关的法律、条约、协定和协议，尽可能充分地提供司法协助。
> [...]

第 18 条的第 1 款和第 2 款中规定了国际合作的一般原则。[2468] 这些原则既适用于网络犯罪调查，也适用于传统调查。欧洲理事会《网络犯罪公约》中也包含有类似的规定。

> **第 18 条.** 相互司法协助
> [...]
> 3. 可为下列任何目的请求，依据本款之规定给予司法协助：
> (a) 向个人获取证据或陈述；
> (b) 送达司法文书；
> (c) 执行搜查和扣押，并实施冻结；
> (d) 检查（验）物品和场所；
> (e) 提供资料、物证以及鉴定结论；
> (f) 提供有关文件和记录的原件或经核证的副本，其中包括政府、银行、财务、公司或营业记录；
> (g) 为取证目的而辨认或追查犯罪所得、财产、工具或其他物品；
> (h) 为有关人员自愿在请求缔约国出庭提供方便；
> (i) 不违反被请求缔约国本国法律的任何其他形式的协助。
> [...]

《公约》第 18（3）款中明确规定了司法协助请求的具体内容。列表中综合给出了从取证开始直至追查犯罪所得的一系列问题。如前文所述，UNTOC 公约并未就与数据相关的请求作出明确的规定，例如通信拦截和数据保护的请求。但是，第 18 条第 3(i)款开放了对其他请求的规定，因此 UNTOC 同样可适用于与数据相关的请求。然而，《公约》只是从总体意义上探讨司法协助请求具体规定的益处，与包含专项请求的区域性措施（例如欧洲理事会《网络犯罪公约》）相比，通常只涉及到各国法律中的程序性措施，却并未就司法协助请求定义明确具体的程序。

第 18 条. 相互司法协助

[...]

4. 缔约国主管当局如认为与犯罪事项有关的资料可能有助于另一国主管当局进行或顺利完成调查和刑事诉讼程序，或可促成其根据本公约提出请求，则在不影响本国法律的情况下，可无须事先请求而向另一国主管当局提供此类资料。

5. 根据本条第 4 款之规定提供此类资料，不应影响提供资料的主管当局本国所进行的调查和刑事诉讼程序。接收资料的主管当局应遵守对资料保密的要求，即使只是暂时保密的要求，或对资料使用的限制。但是，这不应妨碍接收缔约国在其诉讼中披露可证明被控告人无罪或罪轻的资料。在这种情况下，接收缔约国应在披露前通知提供缔约国，而且如果提供缔约国要求，还应与其进行磋商。如果在例外情况下不可能事先通知，接收缔约国应毫不迟延地将披露一事通告提供缔约国。

[...]

第 18 条第 4 款和第 5 款之规定论述了情报共享的问题。其中规定了国际合作的一种形式[2469]，这种合作发生在自愿的基础之上，不需要求资料接受方提交司法协助请求。[2470] 规定中包含关于刑事犯罪的资料，例如在某次调查中发现的位于另一国家的儿童色情业潜在消费者的资料。特别的，在复杂的联合调查中，如果正式的司法协助措施既耗时又有可能妨碍后续的调查，那么执法机构往往会转而去寻求非正式的合作手段。然而，如果资料接受国能够依靠自身收集到所有的相关资料，那么资料共享也只能充当某种替代手段。在其他所有情况下，为了能够保证监管链的完整，通常无论如何都需要正式的合作。在对是否应将国际合作从正式请求转变为自发的资料共享的争论中，重要的是应时刻谨记应开发正式程序以保护国家的主权完整以及被控告人的权利。因此，资料共享不应规避司法协助的法理性结构。

第 18 条. 相互司法协助

[...]

6. 本条款之各项规定，不得影响任何其他用于规范司法协助问题的双边或多边条约所规定之义务，无论是整体或是部分。

7. 如果有关缔约国不受其他司法协助条约之约束，那么本条之第 9 款至第 29 款应适用于依据本条提出之请求；如果有关缔约国有此类条约的约束，则适用条约之相应条款，除非这些缔约国同意代之以适用本条第 9 款至第 29 款。大力鼓励各缔约国在这些条款有助于合作时予以适用。

8. 缔约国不得以银行保密为由拒绝提供本条所规定之司法协助。

9. 缔约国可以并非双重犯罪为由拒绝提供本条所规定之司法协助。但是，被请求缔约国可在其认为适当时在其斟酌决定的范围内提供协助，而不论该行为依据被请求缔约国本国法律是否构成犯罪。

10. 在一缔约国境内羁押或服刑之人，如果被要求到另一缔约国进行辨认、作证或提供其他协助，以便为就与本公约所涵盖之犯罪有关的侦查、起诉或审判程序取得证据，在满足以下条件的情况下，可予移送：

(a) 该人在知情后自愿表示同意；

(b) 经双方缔约国主管当局同意，但必须符合这些缔约国认为适当的条件。

11. 就本条第 10 款而言：

(a) 该人被移送前往的缔约国应有权力和义务羁押被移送人，除非移送缔约国另有要求或授权；

(b) 该人被移送前往的缔约国应毫不迟延地履行义务，按照双方缔约国主管当局事先达成的协议或其他协议，将该人交还移送缔约国羁押；

(c) 该人被移送前往的缔约国不得要求移送缔约国为该人的交还启动引渡程序；

(d) 该人在被移送前往的国家的羁押时间应折抵在移送缔约国执行的刑期。

12. 除非按照本条第 10 款和第 11 款移送该人的缔约国同意，无论该人国籍为何，均不得因其在离开移送国国境前的作为、不作为或定罪而在被移送前往的国家境内使其受到起诉、羁押、处罚或对其人身自由实施任何其他限制。

[...]

第 18 条第(6)–(12)款规定了司法协助的程序性特征。对于网络犯罪案件应重点关注其中的第 8 款和第 9 款之规定。第 9 款之规定使各国能够以并非双重犯罪（在两国领域内皆构成犯罪）为理由拒绝协助请求。此点对于协调当前有限的关于网络犯罪的独立刑事规定（例如欧洲理事会《网络犯罪公约》）方法的范围尤为重要。截至 2010 年中段，只有 30 个国家就网络犯罪问题批准了此合约并为之确定了相应的最低标准。这可能会妨碍基于 UNTOC 公约的国际合作。

第 18 条．司法协助

[...]

13. 每一缔约国均应指定一中心机构，使其负责并有权接收司法协助请求，或执行此请求或将其转交主管当局执行。如缔约国有实行独立司法协助制度的特区或领土，可为该特区或领土另行指定一对其行驶同种职能的中心机构。中心机构应确保其所收到的请求能够得以迅速而妥善的执行或转交。中心机构在将请求转交某一主管当局执行时，应促使该主管当局迅速而妥善地执行请求。各缔约国应在交存本公约批准书、接受书、核准书或加入书时，将为此目而指定的中心机构通知联合国秘书长。司法协助请求以及与之相关的任何通信资料均应递交缔约国指定的中心机构。此项规定不得损害缔约国要求通过外交渠道，以及在紧急和可能的情况下，经有关缔约国同意通过国际刑事警察组织向其传递这种请求和通信资料的权利。14. 协助请求应以被请求缔约国能够接受的语言以书面形式提交，或在可能情况下，以能够生成书面记录的任何形式提出，但是必须使该缔约国能够鉴定其真伪。各缔约国应在其交存本公约批准书、接受书、核准书或加入书时，将其所能接受的语言通知联合国秘书长。在紧急情况下，如经有关缔约国同意，请求可以口头方式提出，但应在此后立即加以书面确认。

15. 司法协助请求书应载有：

(a) 提出该请求的机构；

(b) 请求所涉及的侦查、起诉或审判程序的事由和性质，以及进行此项侦查、起诉或审判程序的当局的名称与职能；

(c) 有关事实的概要情况，为送达司法文书而提出的请求例外；

(d) 对请求协助的事项以及请求缔约国希望遵循的特定程序的详细说明；

(e) 可能时，任何有关人员的身份、所在地和国籍；

(f) 搜寻证据、资料或要求采取行动的目的。

16. 被请求缔约国可要求提供按照其本国法律执行该请求所必需的或有助于执行该请求的补充资料。

[...]

第 18 条第(13)–(16)款定义了司法协助请求的形式与内容以及其通信渠道。就通信渠道而言，《公约》中遵循自中心机构到中心机构传递请求的理念[2471]。《公约》强调了此过程在确保请求能够快速和适当执行中的重要性。各中心机构所承担的角色可能会有所差异，其职权范围从直接参与

请求的处理和执行，延伸至将其转发至主管当局。《公约》将是否需要通过外交渠道传递请求的权限保留给各国。选择此渠道则意味着一个漫长的过程，繁冗的外交程序会显著降低传递的速度，对诸如通信数据保护之类的紧急措施的阻碍尤为严重。与欧洲理事会《网络犯罪公约》不同，[2472] UNTOC 公约并未定义加急合作（expedited cooperation）的手段，而是对紧急案件规定了一套全面的程序。如果请求国同意，可将国际刑警组织（国际警察组织）用作沟通渠道。为了便于另一国家相关机构进行身份认证，联合国毒品和犯罪问题办事处（The United Nations Office on Drugs and Crimes, UNODC）负责维护一在线名录。[2473] 名录中包含请求国签发机构和中心当局的详细资料，通信渠道以及其他相关信息。[2474]

在提交请求时，要求申请书必须符合第 14 和 15 款所定义的正式格式。口头的请求只有在紧急案件中才被允许，且需要随后提交书面请求。缔约国申请加入公约的报告表明，虽然多数国家都通过立法的形式要求 MLA 请求必须为书面形式，但还是有少数的国家认可通过电子邮件转发的临时预先请求。[2475]在这一点上，UNTOC 与欧洲理事会《网络犯罪公约》是不同的，后者鼓励各国在紧急案件中使用电子通信手段。[2476]为了能够确保请求书的完备性，UNODC 提供了一套用于起草此类请求书的软件（司法协助请求写作工具）。[2477]

第 18 条．相互司法协助

[…]

17． 请求应根据被请求缔约国本国法律执行。在不违反被请求缔约国本国法律的情况下，如有可能，应遵循请求书中列明之程序执行。

18． 当在某一缔约国境内的某人需作为证人或鉴定人接受另一缔约国司法当局之询问，且该人不可能或不愿到请求国出庭，则前一缔约国可应另一缔约国之请求，在可能且符合本国法律基本原则的情况下，允许以电视会议方式进行询问，缔约国可商定由请求缔约国司法当局进行询问，且询问时应有被请求缔约国司法当局在场。

19． 未经被请求缔约国的事先同意，请求缔约国不得将被请求缔约国提供的资料或证据转交或用于请求书所述之外的侦查、起诉或审判程序。本款之规定不妨碍请求缔约国在其诉讼中披露可证明被告人无罪或罪轻的资料或证据。就后一种情形而言，请求缔约国应在披露之前通告被请求缔约国，如果对方有所要求，还应依此要求与被请求缔约国磋商。如在例外情况下不可能事先通知时，请求缔约国应毫不迟延地将披露一事通告被请求缔约国。

20． 请求缔约国可要求被请求缔约国对其所提出之请求及其内容保密，但为执行请求所必需时除外。如果被请求缔约国不能遵守保密要求，应立即通知请求缔约国。

21． 在下列情况下，可拒绝提供司法协助：

(a) 请求未按本条之规定提出；

(b) 被请求缔约国认为执行请求可能损害其主权、安全、公共秩序或其他基本利益；

(c) 假如被请求缔约国当局依其管辖权对任何类似犯罪进行侦查、起诉或审判程序时，其本国法律将会禁止其对此类犯罪采取被请求的行动；

(d) 同意此项请求将违反被请求国关于司法协助的法律制度。

22． 缔约国不得仅以犯罪又被视为涉及财政事项为由拒绝司法协助请求。

23． 拒绝司法协助时应说明理由。

24． 被请求缔约国应尽快执行司法协助请求，且应尽可能充分的考虑到请求缔约国所建议并说明了理由的任何最后期限，理由最好是在请求书中给出。被请求缔约国应依请求缔约国的合理要求就其处理请求的进展情况作出答复。请求国应在其不再需要被请求国提供所寻求的协助时迅速通知被请求缔约国。

25． 被请求缔约国可以司法协助妨碍正在进行的侦查、起诉或审判为由而将其暂缓执行。

26. 在根据本条第 21 款拒绝某项请求或根据本条第 25 款暂缓执行请求事项之前，被请求缔约国应与请求缔约国协商，以考虑是否可在其认为必要的条件下给予协助。请求缔约国如果接受附有条件限制的协助，则应遵守相关的条件。

27. 在不影响本条第 12 款之适用的情况下，应请求缔约国之请求而同意到请求缔约国就某项诉讼作证或为某项侦查、起诉或审判程序提供协助的证人、鉴定人或其他人员，不应因其离开被请求缔约国领土之前的作为、不作为或定罪而在请求缔约国领土内被起诉、羁押、处罚，或在人身自由方面受到任何其他限制。如该证人、鉴定人或其他人员已得到司法当局不再需要其到场的正式通知，在自通知之日起连续十五日内或在缔约国所商定的任何期限内，有机会离开但仍自愿留在请求缔约国境内，或在离境后又自愿返回，则此项安全保障即不再有效。

28. 除非有关缔约国另有协议，执行请求的一般费用应由被请求缔约国承担。如执行请求需要或将需要支付巨额或特殊性质的费用，则应由有关缔约国进行协商，以确定执行该请求的条件与细则以及费用承担的方式。

29. 被请求缔约国：

(a) 应向请求缔约国提供其所拥有的根据其本国法律可向公众公开的政府记录、文件或资料的副本；

(b) 可自行斟酌决定全部或部分地或按其认为适当的条件向请求缔约国提供其所拥有的根据其本国法律不允许向公众公开的任何政府记录、文件或资料的副本。

30 缔约国应尽可能视需要考虑，缔结有助于实现本条目的、具体实施或加强本条规定的双边或多边协定或协议的可能性。

6.6.5 欧洲理事会《网络犯罪公约》

《欧洲理事会《网络犯罪公约》》（下文简称“网络犯罪公约”）在其第 23 条至第 35 条关注了国际合作日益增加的重要性。

国际合作的一般原则

欧洲理事会《网络犯罪公约》第 23 条就其成员国之间在网络犯罪调查问题上的国际合作定义了三条一般原则。

第 23 条 – 关于国际合作的一般原则

为了涉及计算机系统和数据的犯罪调查或相关行动、或为了电子形式犯罪证据的收集，各缔约方应依据本章（第 III 章）之规定，通过将与犯罪事务国际合作相关的国际性措施、在统一立法或互惠（相互适用性）立法的基础上达成的协议，以及国内法规等的应用程度最大化，加强彼此之间的相互合作。

首先，公约期望各成员国能够在国际调查中在尽可能广阔的范围内提供相互合作。此项义务的规定反映了国际合作在网络犯罪调查中的重要性。此外，第 23 条还重点强调，一般原则不是仅仅适用于网络犯罪调查，而是适用于所需收集证据为电子形式的任何调查。其涵义同时包含了网络犯罪调查和传统案件的调查。如果一谋杀案嫌犯在国外使用电子邮件服务，那么将适用第 23 条之规定，应对主机提供商存储的数据展开必要的调查。[2478] 第三条原则强调的是，本公约中处理国际合作问题的规定，并不能代替国际协议中关于司法协助和引渡的规定，或者是国内法规中关于国际合作的相关规定。《网络犯罪公约》的起草人强调指出，司法协助通常应通过司法协助相关条约或类

似协议的应用予以执行。因而，《网络犯罪公约》的目的，并不是意图单独为司法协助建立一通用体制。所以，只有在现有条约、法规和协议确实未包含此类规定时，才要求双方确立某种法律基础以确保《网络犯罪公约》所定义之国际合作能够得以顺利执行。[2479]

引渡

侨民的引渡至今仍是国际合作中最大的难题之一。[2480] 引渡请求经常会导致保护公民的需要与支持在国外正在进行的调查的需要二者之间的冲突。《网络犯罪公约》第 24 条规定了引渡的基本原则。与第 23 条不同，此条之规定仅限于《网络犯罪公约》所论及之罪犯，且不适用于罪行较轻的案件（剥夺人身自由至少一年）[2481]。为了避免相关各方就保留权利问题而引发冲突，第 24 条之规定是基于双重犯罪原则的。[2482]

第 24 条– 引渡

1a. 本条款适用于依据本《公约》第 2 条至第 11 条所确定之犯罪行为在各缔约方之间的引渡，其条件是依据双方之法律，其犯罪行为可依法剥夺自由的最长期限至少为 1 年，或者更为严厉的处罚。

b. 如果依据适用于双边或多边的，基于在统一立法或互惠（相互适用）性立法的基础上达成之协议或者引渡条约，包括《欧洲引渡公约》（ETS No. 24），可应用不同的最低处罚标准，那么应适用达成之协议或条约下的最低处罚。

2. 本条款第 1 款所记述之违法行为，均应被视作包含在缔约方之间现行的、双边或多边的、任何引渡条约中的可引渡的犯罪行为。各缔约方承诺将该犯罪视为缔约方间缔结的任何引渡条约中的可引渡的犯罪。

3. 如果依据现有条约实施有条件引渡的一缔约方接收到来自另一未签署此引渡条约的另一方的引渡请求，该缔约方可将本《公约》视为是本条第 1 款所记述之任何犯罪的引渡的合法依据。

4. 当前不存在有条件引渡条约之各缔约方，应将本条第 1 款所记述之犯罪行为视为可引渡的犯罪行为。

5. 引渡应服从被请求缔约方的法律或可适用的引渡条约所规定之条件，包括被请求缔约方可以拒绝引渡的理由。

6. 如果仅仅因为被请求引渡者的国籍，或者是因为被请求方认为其对犯罪行为拥有司法管辖权，而拒绝与本条第 1 款所记述之犯罪行为相关的引渡，那么出于诉讼目的，应请求方之要求，被请求方应将案件提交其主管当局，并适时将最终结果告知请求方。主管当局则应依据己方之决定，按照请求方的法律以与之具有可比特性的任何其他犯罪行为的相同方式实施调查和诉讼。

7a. 每一缔约方，在签署或提交认可、接受、批准或正式加入时，应将在无条约情况下负责提出或接受引渡请求或临时拘捕请求的各主管当局的名称和地址，告知欧洲理事会秘书长。

b. 欧洲理事会秘书长将建立并及时更新各缔约方指定之主管机构的登记记录。各缔约方在任何时候均应确保记录中所存之详细信息都是正确的。

相互司法协助的一般原则

关于司法协助问题，第 25 条在第 23 条所阐述之原则的基础上进行了补充。其中的第 3 款是第 25 条中至关重要的规则之一，此款高度强调了快速通信在网络犯罪调查中的重要性。[2483] 正如我们先前所指出的，许多国家层面的网络犯罪调查，其失败的原因就在于调查花费了太长的时间，因而在采取必要的程序性措施进行保护之前，重要的数据已被删除。[2484] 由于在执法机构间正式请求的通信过程需要花费很多的时间，所以需请求司法协助的调查通常需要更长的时间。《网络犯罪公约》试图通过高度强调推动快速通信手段应用的重要性，致力于解决该问题。[2485]

第 25 条—关于相互协助的一般原则

1. 为了涉及计算机系统和数据的犯罪调查或相关行动、或为了电子形式犯罪证据的收集，缔约方应在最大可能的范围上向另一方提供司法协助。

2. 每一缔约方还应采取必要的立法手段和其他措施来履行第 27 条至第 35 条所规定之义务。

3. 在紧急情况下，每一缔约方均可通过快速通信手段，包括传真或电子邮件，提出司法协助请求或其他通信请求。使用快速通信手段应保证其能够提供适当的安全保密性和可鉴别性（包括在必要时可使用密码加密），且在受请求缔约方要求下提供后续正式确认。被请求缔约方应接收到通过任何此类快速通信手段传递之请求后对此做出回应。

4. 除非在本章其他条款中另有特别规定，司法协助应服从于被请求缔约方本国法规或可适用之司法协助条约所规定之条件，包括被请求缔约方可以拒绝合作之理由和依据。就本公约第 2 条至第 11 条所记述之犯罪行为，被请求缔约方不得仅仅以此请求涉及之犯罪被视为经济犯罪为理由而行使权力拒绝司法协助。

5. 当依据本章之规定，被请求缔约方同意在双重犯罪的基础上实施有条件司法援助时，如果依据被请求缔约方之法律可认定正在寻求协助之犯罪行为是刑事犯罪，那么无论双方之法律是否将此犯罪归为相同类别或者是请求缔约方是否使用相同的术语来命名此犯罪，均应认为此条件是可满足的。

在国家层面上进行的网络犯罪调查期间，可能会发现涉及另一国家的犯罪行为的线索。例如，如果执法机构正在调查一儿童色情案件，那么他们可能会发现来自其他国家的，参与了儿童色情交易的恋童癖者的信息。[2486] 在此情况下，第 26 条规定了执法机构在不危害其自身调查的前提下，必须通告外国执法机构的相关义务。[2487]

第 26 条— 主动信息

1. 当某缔约方认为在其本国调查架构内所获知之信息的披露，可能有助于接收方起动或完成与依据本《公约》所确定之犯罪行为有关的调查或诉讼时，或者当其认为接收方可依据本章之规定提出合作请求时，在其本国法律限制范围内且无需事先申请，缔约方可以向另一缔约方转寄上述信息。

2. 在提供此类信息之前，提供信息的缔约方可要求信息接受方对其保密或只可依据规定条件使用。如果信息接受方不能遵守上述要求，应立即通告信息提供方，后者随后将决定是否仍为其提供信息。如果信息接受方接受有附加条件的信息，则该缔约方应受相应条件的约束。

正如前文所指出的，关于以主动信息替代司法协助仍有许多值得关注的问题。信息共享只有在信息接受国能够依靠自身搜集到全部的相关证据时才能够发挥其应有作用。在其他所有情况下，为了能够确保监管链的完整，通常无论如何都需要正式的合作。在对是否应将国际合作自正式请求转变为自发的情报交换的争议中，必须时刻谨记应开发正式程序以保护国家主权完整以及被控告人的权利。因此，信息共享不应规避司法协助的法理性结构。

第 26 条中最重要的规定之一就是关于信息的机密性。考虑到许多的调查都只有在罪犯没有察觉到正在被调查时才能够得以顺利进行，那么第 26 条之规定使信息提供方能够要求接收方保证其所传递信息的机密性。如果对方无法保证其机密性，那么提供方可以拒绝提供信息。

在没有适用国际协议时请求相互司法协助的程序

与第 25 条、第 27 条基于相同的理念，即司法协助应通过相关条约以及类似协议的应用来实施，而不是仅仅依赖于《网络犯罪公约》。因而，《网络犯罪公约》的起草者决定，不在《公约》内单独建立司法协助的强制体系。[2488] 如果已有其他可适用的措施，那么第 27 条和第 28 条之规定与某一具体的请求并不相关。只有在其他规定均不适用的情况下，第 27 条和第 28 条才会提供一套可用于实现司法协助请求的机制。

第 27 条所规定的最为重要的内容，就是包含了为司法协助请求建立指定联络点的义务[2489]。按其规定之要求，各联络点之间应可实现直接通信[2490]，并由欧洲理事会秘书长创建所有联络点的数据库，以避免冗长的程序。

此外，第 27 条还规定了关于援助请求的限制。特别是，关于政治犯罪行为，或者是认为合作会损害其国家主权、安全、公共秩序或其他根本利益的，《网络犯罪公约》的缔约国可以拒绝合作请求。

在此，《网络犯罪公约》的起草者考虑了两个方面的需求：一方面是需要使缔约国能够拒绝就某些特定案件的合作，而在另一方面又指出各缔约国应在限定范围内行使其拒绝合作的权利，其目的就是为了避免与先前所确定之原则的冲突。[2491] 因而，从狭义的角度定义术语“其他根本利益”是尤为重要的。《网络犯罪公约》解释性报告中指出，此限定可理解为如果合作可能给被请求国带来根本性的困难。[2492]站在条约起草者的观点，关于不适当数据保护法律的具体事务不应被视为“根本利益”。[2493]

有关临时性措施的相互司法协助

第 28 条至第 33 条是《网络犯罪公约》程序性措施的具体反映。[2494] 《网络犯罪公约》中包含许多意图用于改善其成员国调查状况的程序性措施。[2495] 就国家主权原则而言[2496]，这些措施只能被用于国家层面的调查。[2497]如果调查人员认为需要在其国家领土范围以外收集证据，他们就需要请求司法协助。除第 18 条之规定外，第 16 条至第 21 条所规定的每一项措施，在第 28 条至第 33 条都有着与之相应的规定，在接受外国执法机构的请求后，本国执法机构可应用这些具体的程序性措施。

程序性措施	相应的ML规定
第 16 条 – 现存计算机数据的加速保护[2498]	第 29 条
第 17 条 – 通信数据的加速保护与部分披露[2499]	第 30 条
第 18 条 – 制作[2500]	无
第 19 条 – 现存计算机数据的搜查与查封[2501]	第 31 条
第 20 条 – 通信数据的实时收集[2502]	第 33 条
第 21 条 – （通信）内容数据的拦截与侦听[2503]	第 34 条

现存计算机数据的跨境访问

除纯粹的映射程序性规定外，《网络犯罪公约》的起草者还论述了在何种情境之下，才允许执法机构访问那些既非储存于其国境之内又非其境内人员控制的计算机数据。最终，他们仅就下述两种情境下无需司法协助请求即可由执法机构实施调查达成一致意见。[2504]进一步的协议始终不可能达成，[2505]即使是所达成的解决方案至今仍受到欧洲理事会各成员国的批评。[2506]

允许执法机构访问其境外储存的数据的案件情境包括：

- 公众可访问的信息资料；和/或
- 访问已经得数据实际控制人的同意。

第 32 条–在获得同意或可公开访问的情况下越境访问现存计算机数据

未经另一缔约方的授权，某缔约方可以：

a 访问可公开获得（开源）的现存计算机数据，而不管该数据的地理定位；或

b 如果该缔约方获得了相应人员的合法、自愿的同意（该人员拥有通过计算机系统披露其数据之合法权限），可经其领土范围内的计算机系统，访问或接收位于另一缔约方领土范围内的现存计算机数据。

第 32 条中既未规定其他的跨境访问形式，但同时也未阻止。[2507]

第 32 条指出，如果相关数据对公众开放，则允许国外执法机构访问此信息。公众可访问信息的一个实例就是将信息发布到无访问控制（例如密码）的网站。与其他用户不同，如果不允许调查人员访问这些网站，可能就会严重阻碍他们的工作。因此，第 32 条所规定的第一种情境能够被广泛接受。

允许调查人员访问其境外现存计算机数据的另一情境，就是调查人员在经得拥有披露这些数据合法权限的人员的合法、自愿同意后。这种授权访问方式受到了严厉的批评。[2508]

人们广泛关注的问题之一，就是现行规定的措辞可能与国际法基本原则相抵触的事实。[2509] 基于国际法原则，调查人员在调查期间必须尊重被调查国的国家主权。[2510] 在未经所在国主管机构的同意时，尤其不允许他们在另一主权国家实施调查。由于涉及国家主权问题，此类授权不仅影响个人权利，还会影响国家利益。因此，是否可对调查人员进行此类授权的决定权并不在个人手中，而是在国家有关当局手中。通过批准签署《网络犯罪公约》，各缔约国放弃了部分原则，允许其他国家实施影响其领土完整的调查。

人们广泛关注的另一问题在于，第 32 条之 b 款中并未定义调查的具体程序。基于规定之文本表述，似乎没有必要对将国内法规中现有的，关于类似的国内调查施加相同的限制。但是有趣的是，在 2000 年初《网络犯罪公约》草案的正文中仍包含有这样的限定，但是在第 22 版草案中已被删除。[2511]

通过第 32 条 b 款之规定，《网络犯罪公约》起草者从根本上违反了本公约司法协助体制的法理性结构。通过第 18 条之规定，《网络犯罪公约》起草者使调查人员能够在国内调查中通过命令的形式要求数据的提交。如果能够授权执法机构可在国际调查中采取此类措施，那么该措施可能早已有充分理由被包含于司法协助上下文中的措施目录。但是，由于《网络犯罪公约》第 3 章中处理国际调查问题相应规定的缺失，使得该项措施无法应用于国际调查中。公约起草者并未通过允许国外调查人员直接联系数据资料的控制人而放弃其法理性结构，而只是简单的贯彻了公约第 3 章之相应规定。[2512]

在 1999 年莫斯科召开的打击跨国有组织犯罪 G8 部长级会议上，现存计算机数据的跨境访问问题同样备受争议。[2513] 本次会议的成果之一，就是集中征集了关于跨境访问的原则。[2514] 这很可能就是《网络犯罪公约》起草者所作规定的原型，因此它们看上去非常相似。

6. 在未提出司法协助请求的情况下越境访问现存数据

虽然这些原则中包含了诸多限制，但是当一国出于下述目的，依据本国法律进行调查时，不需获得另一国家的授权：

(a) 访问公众可访问（开源）的数据，无论此数据地理位置上位于何处；

(b) 如果能够获得依法享有披露该数据权限之人员的合法、自愿同意，访问、搜索、复制或拦截位于另一国家的计算机系统中现存数据；如果本国法律允许发出此类通告，且数据揭示了一违犯被搜索国刑法或其他看似触犯被搜索国利益的案件，搜索国可考虑将其通告被搜索国。

二者之间的主要差异在于第 6 (b)款所规定的通告程序。此规定之目的就是资料共享。然而，在经过少许修改之后，这样一条规定就能够确保受到影响的国家意识到调查是发生在他们自己的版图之内。虽然这样并不能防止与国际法之间的冲突，但是至少能够在某种程度上保证其透明性。

24/7 联络点网络

网络犯罪调查通常需要快速的反应。[2515] 正如前文之解释，特别是在必须利用通信数据确定嫌犯身份时，快速的反应尤为重要，因为这些数据通常在相当短的时间内就会被删除。[2516] 为提高国际调查的速度，《网络犯罪公约》在第 25 条中重点强调了促进加速通信手段的应用的重要性。为了能够进一步提高司法协助请求的效率，《网络犯罪公约》的起草者强制要求各缔约方为司法协助请求指定一联络点，该联络点的有效性应不受时间限制。[2517]《网络犯罪公约》的起草者强调，这些联络点的设立是公约所能够提供的最为重要的措施之一。[2518] 然而，最近的一份已批准加入《网络犯罪公约》各国的 24/7 联络点网络应用情况的综述表明，其应用非常有限。

第 35 条— 24/7 联络点网络

1. 公约的每一缔+约方均应指定一联络点，该联络点应每周 7 天、每天 24 小时均可联络，以确保在进行与计算机系统及数据相关的犯罪调查或起诉，或收集电子形式的犯罪证据时提供即时协助。如其国内法律与实践惯例允许，则此类协助应有助于下列行动直接实施：

a. 提供技术建议；

b. 依照第 29 条和第 30 条提供数据保护；

c. 收集证据、提供法律信息以及定位嫌疑犯；

2 a. 每一缔约方之联系点均应具有与另一缔约方之联系点实现快速通信的能力。

b. 如果缔约方指定之联系点不是缔约方负责国际司法协助或引渡事务之主管机构的组成部门，那么此联系点应确保其能够与上述机构实现快速协调。

3. 为便于联络点网络的正常运行，每一缔约方均应确保为其培训并配备相应人员。

建立 24/7 网络的设想，是在当前 G8 国际组织为国际高技术犯罪和与计算机有关的犯罪所建立的 24 小时联系网络的基础之上提出的。[2519]《网络犯罪公约》的起草者旨在通过 24/7 联络点网络的建立以应对打击网络犯罪所面临的挑战——尤其是那些与数据交换处理[2520]的速度有关的，以及具有国际维度特征[2521]的挑战。此条规定强制要求《网络犯罪公约》各缔约方设立此类联络点，并确保其能够可靠地完成即时响应以及维持其业务运行。为实现此目的，应如《公约》第 34 条第 3 段之规定为联络点培训并配备相应人员。

就此联络点的组建程序，尤其是此组织结构的基本原则等，《网络犯罪公约》给予了各成员国最大的灵活性。《公约》既没有要求组建一个新的机构，也没有明确规定此联络点可以或应该隶属

于哪一现有机构。《网络犯罪公约》的起草者进一步指明如下之事实，即旨在通过 24/7 联络点网络所提供之技术与司法协助，或可为跨境网络犯罪调查的实施提供各种可能的解决方案。

就网络犯罪调查而言，建立联络的主要作用包括以下两点：即通过单一联络点的设置加速通信过程；以及通过授予联络点独立行使实施特定调查的权利加速调查的过程。将上述两功能相结合，就有可能极大提高国际调查的速度，使之达到与国内调查同等的水平。

《网络犯罪公约》第 32 条规定了联络点的最低能力要求。除技术协助和提供法律信息外，联络点主要的任务还包括数据资料的保护、证据的收集以及嫌犯的定位等。

关于此点，需再次重点强调的是，《国际犯罪公约》中并未规定应由哪一机构负责 24/7 联络点的运行。如果负责运营联络点的机构拥有强制命令以保护数据的权力，[2522] 而国外联络点又请求此类保护，那么本地的联络点可发布命令立即采取该措施。如果负责运营联络点的机构自身并不具备强制命令以保护数据的权力，那么联络点应有能力立即联系具有该权限的主管部门以确保能够马上采取措施就是非常重要的了。[2523]

在网络犯罪公约委员会第 2 次会议上，委员会明确提出，申请参与加入 24/7 联络点网络不需签署和批准《网络犯罪公约》。[2524]

2008 年，欧洲理事会出版了《打击网络犯罪国际合作效率分析研究》。[2525] 2009 年，着手开展了对网络犯罪 24/7 联络点运行状况的专项研究。[2526]上述研究的结论之一，就是批准加入《网络犯罪公约》的所有国家，都按照《公约》之要求建立了具有 24/7 联络功能的联络点网络。而其次的结论就是，已建立网络联络点的各缔约国，通常只是将其用于非常有限的目的，例如通信数据的保护。

6.6.6 《斯坦福国际公约草案》中的国际合作

《斯坦福国际公约》草案（下文简称“斯坦福草案”）[2527] 的起草者充分认知到网络犯罪的国际化维度以及相关挑战的重大性。为了能够应对这些挑战，他们在草案中针对国际合作问题加入了一些专项规定。该组规定包括以下条款：

- 第 6 条 – 相互司法协助
- 第 7 条 – 引渡
- 第 8 条– 起诉
- 第 9 条– 临时性补救措施
- 第 10 条– 被控告人的权利
- 第 11 条– 执法合作

此方法非常类似于欧洲理事会《网络犯罪公约》所采用之方法。二者之间的主要差异在于如下之事实，那就是与《斯坦福草案》相比，《网络犯罪公约》所作之规定更为严格、更加复杂，限定也更为清晰明确。正如《斯坦福草案》的起草者所指出的，《网络犯罪公约》之方法更具实用性，因而在实际运用方面具有某些明确的优势。[2528] 而《斯坦福草案》的起草者决定遵循另一不同的方法，按照他们的预测，新技术的推行必将带来一些新的困难。因此，草案中只是规定了一些通用的措施，而不是进一步将其具体化。[2529]

6.7 互联网服务提供商的责任

参考书目（节选）： *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Luotonen*, Web Proxy Servers, 1997; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html; *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf; *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003.

6.7.1 引言

即使罪犯只是独立作案，其网络犯罪的实施也会自然而然的牵涉众多的人员与交易。由于互联网的结构特征，即使只是一封简单的电子邮件的传输，也还是需要众多提供商为其提供服务。[2530] 除电子邮件服务提供商外，邮件的传输还涉及网络访问提供商，以及将电子邮件逐级转发至接收者的路由器。其情形与下载包含儿童色情内容的影片非常类似。整个下载过程涉及上传图片的内容提供商（例如某网站）、为网站提供存储介质的主机托管服务提供商、负责将文件转发至用户的路由器，以及最后使用户能够访问互联网的网络提供商。

因为这种涉及多方的牵连关系，只要罪犯利用其所提供的服务实施犯罪行为，那么互联网服务提供商（ISP）必然就会成为此类案件犯罪行为调查的焦点。[2531] 导致事态发展至此的主要原因之一就在于，即使罪犯是在国外实施其犯罪时，在不违反国家主权原则的前提下，位于本国国界之内的各类提供商自然就会成为犯罪调查的适宜对象。[2532]

事实包含另个方面：一方面是如果没有各类服务提供商的参与，罪犯根本无法实施犯罪；而在另一方面则是提供商通常没有能力阻止这些犯罪。如此事实最终导致了这样一个问题，也就是是否需要对互联网服务提供商应承担的责任作出某种限制。[2533] 该问题的答案对于 ICT（信息通信技术）基础设施的经济发展是非常关键的。如果在其正常运作模式下能够避免造成犯罪，那么服务提供商就只需关注其自身业务的运营。此外，执法机构对此问题也有着强烈的兴趣。执法机构的工作经常需要依赖于互联网服务提供商的合作。这又会引发诸多问题，因其用户的行为而限制互联网服务提供商应承担的责任，可能会对 ISP 对网络犯罪调查的合作与支持，以及真正意义上的预防犯罪等产生影响。

6.7.2 美国方法

一方面需要服务提供商积极参与犯罪调查，而另一方面又需要限制其因第三方之行为而承担犯罪责任的风险，对此可采取不同的方法在二者之间做出平衡。[2534] 通过立法途径在二者之间做出平衡的实例可见于 USC（美国法典）第 17 卷第 512 条（a）和（b）款。

第 512 段.关于在线资料的责任限制

***(a)* 短暂的数字网络通信**

除如（j）项所规定之情形外，如果符合下述之条件，服务提供商无需为通过其所控制或运营之系统或网络传输的资料，或因在此资料的传输、路由或提供链接期间资料的中转存储和暂时存储，因服务提供商之传输、路由或为资料提供链接而造成的版权侵犯，而承担货币赔偿、禁令赔偿的或其他公平赔偿之责任—

(1) 资料的传输是由服务提供商之外的人员发起，或者是在其操作指示下启动；

(2) 资料的传输、路由、连接的提供或储存，是通过某自动技术过程实现，其间无需服务提供商作出资料选择；

(3) 除自动响应其他人员之请求外，服务提供商并未选择资料的接收者；

(4) 服务提供商在此资料在系统或网络中转存储或暂时存储期间，未出于为预期接收者之外的任何人提供常规访问的目的而保留其副本，也并未出于为预期接收者提供长期访问（超过其传输、路由或链接提供的合理必要时间）的目的而保留其副本；且

(5) 资料通过系统或网络传输期间，服务提供商未对其内容进行任何修改。

***(b)* 系统缓存**

(1) 责任限制。— 除如（j）项所规定之情形外，在下述情况下，系统缓存服务提供商无需为其所控制或运营之系统或网络中因资料的中转存储和暂时存储所造成的版权侵犯，而承担货币赔偿、禁令赔偿的或其他公平赔偿之责任 —

(A) 此在线资料是由服务提供商之外的人员上传至网络的；

(B) 资料是自本款（A）项所述之人员处通过系统或网络传输至本款（A）项所述人员之外的人员，且传输是在后者的操作指示下进行方向上；

(C) 资料的存储是通过某自动技术过程完成，存储的目的是为了在本条（B）款所述之资料传输完成后，如符合（B）款所规定之条件，为系统或网络中请求访问（A）款所述之人员提供的资料的用户提供访问，如果第*(2)*段中所述条件得到满足。

[…]

此项规定是基于 1988 年签署生效的《千禧年数字版权法案》（DMCA）的。[2535] 通过建立某种安全港体制，DMCA 将特定服务提供商因第三方违反版权法而需承担的责任排除在外。[2536] 关于此点，首先需要强调的就是，并非所有的提供商都受此限制之约束。[2537] 此项限制只适用于服务提供商[2538]和缓存服务提供商。[2539] 此外，还需重点指出的是，该责任是与特定的要求相联系的。就服务提供商而言，对其要求包括：

- 资料的传输是由服务提供商之外的其他人员发起，或者是在接受其指令后发起；
- 传输的执行是通过某自动化技术处理而非服务提供商选择资料；
- 服务提供商确实没有选择资料的接收方；
- 在资料中转存储和暂时存储期间，服务提供商并未出于为接收方之外的其他人提供正常访问的目的，而在系统或网络中保留资料副本。

另一种互联网服务提供商责任限制的实例可见于 USC 第 47 卷第 230（b）段，此款之规定是基于《通信规范法案》的[2540]：

> **第 230 段.保护私人阻塞和屏蔽不恰当资料**
> […]
> **(c)保护阻塞和屏蔽不恰当资料的“见义勇为者”**
> (1) 发布者或发言人处理
> 在任何交互式计算机服务中，无论服务提供商还是用户，均不得被视为由另一信息内容提供商提供之任何信息的发布者或发言人。
> (2) 民事责任
> 在任何交互式计算机服务中，无论服务提供商还是用户均不应为下述原因而承担责任：
> (A) 出于诚信目的，为限制或禁止访问被提供商或用户视为淫秽、下流、色情、丑恶、过于暴力、扰乱或有伤风化的资料而自愿采取的任何行动，无论在此类资料是否受到宪法保护；或者
> (B) 为确保或通告内容提供商或其他人员采取技术手段限制访问前款所述之资料而采取的任何行动。
> […]

USC 第 17 卷第 512（a）段和第 47 卷第 230（b）段所述方法共同具备的特点就是，二者都是针对于特定的提供商群体和某专业领域的法案。因而，我们将在本章的剩余部分概要评述为欧盟所采纳的立法途径，此方法遵循更广义的概念。

6.7.3 欧盟《电子商务指令》

通过立法途径规范互联网服务提供商之责任的另一实例就是欧盟的电子商务指令。[2541] 面对源自互联网之国际化维度的挑战，指令的起草者决定开发某种立法标准，以为信息社会的全面发展提供一立法框架，并藉此支持经济全面发展以及执法机构的工作。[2542] 此指令中关于责任的规定是基于分级责任原则的。

指令中包含许多用于限制特定服务提供商应承担之责任的规定。[2543] 具体的限制与提供商所运营之不同服务类别相联系。[2544] 在所有其他无需排除其责任的场合，且除非是其受到其他规章之限制，否则行为人应承担全部责任。指令的动机是为了限制那些提供商预防犯罪之可能性受限的情况下其应承担的责任。可能性受限的原因可能是技术性的。例如，如果不以显著牺牲其速度为代价，路由器本身无法过滤通过其传送的数据，也几乎无法阻碍数据交换的过程。如果能够察觉到犯罪行为的存在，主机托管服务提供商是有能力删除相应数据的。但是，与路由器的情况类似，大型的主机托管服务提供商根本无法控制存储于其服务器上的全部数据。

考虑到其实际控制犯罪行为之能力差异，主机托管服务提供商和网络访问提供商的责任也会有所不同。在这一方面，需要考虑到指令所作之平衡同样是基于当前的技术标准的。截至目前为止，还没有一种工具可用于自动侦测未知的色情图片。随着该领域技术的持续发展，将来可能有必要重新评估提供商的技术能力，并在必要时对此体系作出调整。

6.7.4 网络接入提供商的责任（《欧盟电子商务指令》）

此指令的第 12 条至第 15 条定义了对不同提供商的责任限制程度。基于第 12 条之规定，只要其能够符合第 12 条所规定之 3 个条件，那么网络访问提供商和路由器操作人员的责任即可完全排除。因而，网络访问提供商通常并不需要为其用户所犯之罪行承担责任。但是，此全部责任的排除并未减除服务提供商在接到法庭或行管机构的命令时，采取必要的措施以防止犯罪行为进一步扩大的义务。[2545]

第 4 节：中介服务提供商的责任

第 12 条

–“纯粹传输服务”

1. 如果服务提供商所提供之信息社会服务，包括在通信网络中传输由服务接受者提供的信息，或者是为通信网络提供接入服务，那么各成员国应确保此服务提供商无需对所传输之信息承担责任，其条件是：

(a) 服务提供商不是首先发起传输的一方；

(b) 服务提供商未对传输的接收者作出选择；以及

(c) 服务提供商为对传输的信息进行选择或修改。

2. 本条第 1 款所记述之传输及提供接入的行为包括对所传输信息的自动存储、中转存储和暂时存储，其前提是此行为之目的仅仅是为了在通信网络实施传输，而且信息的存储时间不得超过进行传输所必需的合理时间。

3. 本条之规定，不应影响法院或行管机构根据成员国之法律制度，要求服务提供商终止侵权行为或预防侵权行为的可能性。

此方法与 USC 第 17 卷第 512 (a)段的规定具有一定可比性。[2546] 两规定之目的都是为了明确规定服务提供商的责任，且同时都将责任的限制与类似的要求相联系。二者之间的主要差异在于，欧盟《电子商务指令》第 12 条之规定并非只限于违反版权法，而是将排除责任的范围扩展到关于任何类型的犯罪。

6.7.5 缓存服务提供商的责任（《欧盟电子商务指令》）

术语“缓存服务（Caching）”在本文中用于描述为了减小网络带宽开销和更高效的访问数据而将热门网站之数据存储在本地存储介质中。[2547] 可用于减小网络带宽开销的一项技术就是设置代理服务器。[2548] 通过因先前的访问请求而检索取回并保存于本地存储介质的缓存内容，在缓存范围之内，代理服务器无需与指定服务器（用户输入的域名）建立联系即可为后续的请求提供服务。《指令》的起草者认识到缓存服务重要的经济价值，因而决定：如果提供商能够遵从第 13 条所规定之条件，那么即可排除其因自动暂存而引发的相关责任。其所列条件之一就是提供商就信息的更新应遵从广泛认可的标准。

第 13 条

–“缓存技术”

1. 如果缓存服务提供商所提供之信息社会服务，包括在通信网络中传输由服务接受者提供的信息，只要对信息的存储仅仅是为了使应其他服务接受者之要求而上传的信息能够更有效的传输给他们，各成员国应确保此服务提供商无需对信息的自动、中间性和暂时性存储而承担责任，其条件是：

(a) 提供商没有修改信息；

(b) 提供商在获取信息时遵守了相应条件；

(c) 提供商遵守了关于信息更新的规则，此规则以某种被业界广泛认可和使用的方式确定；

(d) 提供商在对信息的使用中，未干预为业界广泛认可和使用的数据获取技术的合法使用；以及

(e) 提供商在获知位于初始传输来源的信息已自网络中移除，或至该信息的访问途径已被阻断，或者法院或行管机构已命令将此信息移除或阻断的事实后，立即行动以移除或阻断对其所存储之该信息的访问。

2. 本条之规定，不应影响法院或行管机构根据成员国之法律制度，要求服务提供商终止侵权行为或预防侵权行为的可能性。

欧盟《电子商务指令》第 13 条是类似介于美国法理结构和欧洲方法之间的又一实例。欧盟方法可比与 USC 法案第 17 卷第 517 条之(b)款。[2549] 二者的目标都是为了规定缓存服务提供商的责任，而且都将责任限制与类似的要求相联系。就服务提供商的责任而言[2550]，两方法之间的主要区别在于，欧盟《电子商务指令》第 13 条之规定并不仅限于侵犯版权法，而是将各类违法之相关责任均排除在外这一事实。

6.7.6 主机托管服务提供商的责任（欧盟指令）

特别的，就非法内容而言，主机托管服务提供商在犯罪实施中发挥了重要的功能。上传非法内容使之能够有效访问的罪犯，通常并不会将这些内容保存于自己的主机。绝大多数的网站都是保存在主机托管服务提供商所提供的服务器上。意欲经营某一网站的任何人员，都可以从主机托管服务提供商处租用存储空间以存储其网站。一些提供商甚至能够免费提供由广告赞助的网络空间。[2551]

对主机托管服务提供商来说，非法内容的鉴别是一个挑战。尤其是对于那些拥有许多网站的热门提供商，在数量如此众多的网站中手动查找非法内容根本就是不可能的。所以，指令的起草者决定限制主机托管服务提供商的责任。但是，与对网络访问提供商的限制不同，主机托管服务提供商的责任并未被全部排除。如果主机托管服务提供商没有真正察觉到非法活动或非法内容存储于其服务器，那么他是无需承担责任的。在此存在这样一种假定，即服务器上可能存储有非法内容与真正获知存在此类问题不可等同视之。如果主机托管服务提供商已获知关于非法活动或非法内容的确切信息，那么他只有立即删除这些信息才能免于责任追究。[2552] 未能对此立即作出反应的主机托管服务提供商将会因此而被追究责任。[2553]

第 14 条

–主机托管服务

1. 如果托管服务提供商所提供之信息社会服务包括存储由服务接受者所提供之信息，各成员国应确保此服务提供商无需因应接受服务者之要求存储的信息而承担责任，其条件是：

(a) 提供商对违法活动或违法信息不知情，而且就损害赔偿而言，提供商对违法活动或违法信息所显现出的事实或情况毫不知情；或者

(b) 提供商一旦获知或意识到存在此类信息，就马上移除了此信息或阻断了对此信息的访问。

2. 如果服务接受者之行为是在提供商的授权或控制之下，则本条第 1 款之规定不适用。

3. 本条之规定，不应影响法院或行管机构根据成员国之法律制度，要求服务提供商终止侵权行为或预防侵权行为的可能性，也不应影响成员国就移除信息或阻断对信息的访问问题制定相关管理规定的可能性。

第 14 条之规定并不仅适用于那些业务范围限于技术性数据—存储基础设施租赁服务的提供商，同样也适用于类似于拍卖平台竞价托管服务的流行的互联网服务。[2554]

6.7.7 主机托管服务提供商的责任（HIPCAR）

限制托管服务提供商责任的另一方法可见于 HIPCAR（协调 ICT 政策、立法和监管程序）项目行动受益国所开发的立法文本。[2555]

托管服务提供商

30

(1) 如果托管服务提供商所提供之信息社会服务包括存储由服务接受者提供的信息，成员国应确保此服务提供商不因应接受服务者之要求存储的信息而承担责任，其条件是：

(a) 在接到任何政府机构或法院移除其所存储之特定违法信息的命令后，托管服务提供商立即删除了此信息或阻断了对其的访问；或者

(b) 托管服务提供商在通过政府机构命令之外的其他途径获知或意识到关于其所存储之特定违法信息的问题后，迅速通知某政府机构以使其能够对此信息作出定性评估，并在需要时发布命令移除此内容。

(2) 如果服务接受者之行为是在提供商的授权或控制之下，则本条第 1 款之规定不适用。

(3) 如果托管服务提供商在收到依据本条第 1 款之规定发布的命令后移除了相关信息内容，那么应免除其相对于其客户的，应确保服务之有效性的违约责任。

就像欧盟方法第二节第五部分 30(1)段一样，如果托管服务提供商在收到任一政府机构或法院的命令后迅速删除了非法内容，那么依据 HIPCAR 第 30 1(a)段的规定可限制提供商应承担的责任。“迅速”通常是指在少于 24 小时时间之内。[2556] 在欧盟方法第二节第五部分第 30 1(b)段中可发现其与欧盟方法之间的主要差异。与欧盟方法的约束不同，提供商无须确认引发其关注的内容是否被视为非法。如果收到此类通知，其义务首先被限制为将可能的非法内容告知（指定的）政府机构。此项规定的起草者认为，确定内容之性质和发布命令删除相应内容应为相关政府机构的责任。[2557] 如果信息被认定为非法，那么提供商应删除之以免除自身责任。

6.7.8 监管责任的排除（《欧盟电子商务指令》）

在《指令》实施之前，就是否可基于其未尽到对用户行为的监管责任而起诉提供商，在一些成员国仍不明确。除可能会与数据保护规章及电信保密相冲突外，此种责任尤其还可能会给那些存储有成千上万网站的主机托管服务服务提供商带来困难。为避免这些冲突，《指令》将对传输和存储的信息的全部监管责任都排除在外。

第 15 条—不承担监督的一般性义务

1. 在服务提供商提供本指令第 12 条、第 13 条以及第 14 条所规定之服务时，各成员国不得强制要求服务提供商承担监督其传输和存储的信息的一般性义务，也不得强制要求服务提供商承担主动收集表明违法活动的事实或情况的一般性义务。

2. 各成员国可强制要求信息社会服务提供商承担立即向主管政府机构报告其服务接受者进行的非法行为或者提供的非法信息的义务，或者应主管当局之要求，向主管当局提供可以确定与其签署有存储协议的服务接受者之身份的信息的义务。

6.7.9 超链接服务提供商的责任（奥地利 ECC）

超链接服务在互联网中承担着重要角色。超链接的存在，使超链接服务提供商能够引领用户访问指定的在线信息。替代以往必须提供的如何去访问信息的技术细节（例如给出提供这些信息的网站的域名），用户直接点击活动的超链接即可访问此信息。超链接负责向 Web 浏览器发出相应命令以打开预先设定的互联网地址。

在欧盟指令起草期间，对是否需要对超链接服务进行规管进行了激烈的争论。[2558] 起草者最终决定，不强制要求各成员国就超链接服务提供商的责任而协调其法规。而是代之以某种复查程序，以确保能够对超链接服务和定位工具服务提供商责任的相关建议加以考虑。[2559] 在未来对超链接服务提供商责任之规定进行修订之前，各成员国可自由开发本国的解决方案。[2560] 一些欧盟成员国已决定就超链接服务提供商的责任作出专门的规定。[2561] 这些国家将超链接服务提供商的责任建立在与欧盟指令就托管服务提供商的责任所作之规定同一原则的基础之上。[2562] 此方法是在将主机托管服务提供商和超链接服务提供商之情形进行比较的基础上而得出的逻辑推理结果。在上述两种情况下，服务提供商均可控制非法信息，或者至少能够控制至此信息的链接

此方法的实例可见于奥地利 ECC（电子商务法案）之第 17 节[2563]

《电子商务法案》（奥地利）第 17 节 – 超链接服务提供商的责任

(1) 通过提供电子链接使第三方能够访问在线信息的提供商，无需对链接指向之信息负责，其条件是：

1. 提供商并未真正获知引发损害赔偿要求的非法活动或信息的存在，也未察觉此事实或情况已使服务提供商之活动或信息看似非法；或
2. 在获知或察觉此问题后，迅速行动以删除此电子链接。

6.7.10 搜索引擎提供商的责任

搜索引擎服务提供商提供的搜索服务可通过规定某些条件以识别用户感兴趣的文件。搜索引擎将自动搜索匹配用户输入条件的相关文件。在互联网的顺利发展中，搜索引擎充当了重要的角色。已上传发布至网站但并未列入搜索引擎索引的内容，只能为那些意图访问此内容且已知其完整 URL（统一资源定位符）的用户所访问。*Introna/Nissenbaum* 在其研究中指出："任何人都可以毫好不夸张的说，要想生存就必须被某搜索引擎索引。"[2564]

关于搜索引擎，欧盟指令中并未包含定义搜索引擎运营商责任的标准。因此，一些欧盟国家决定就搜索引擎服务提供商的责任作出专门的规定。[2565] 与超链接服务的情况不同，并非所有的国家都将其规定建立在同一原则的基础之上。西班牙[2566]和葡萄牙[2567]将其关于搜索引擎运营商责任的规定建立在指令第 14 条之规定的基础之上，而奥地利[2568] 却将其责任限制建立于第 12 条的基础之上。

《电子商务法案》（奥地利）第 14 条 – 搜索引擎运营商的责任

(1) 提供搜索引擎或其他电子工具以搜索由第三方提供之信息的服务提供商，在以下条件下无需为此信息承担责任：

1. 提供商未发起传输；
2. 提供商未选择传输的接收方；且
3. 提供商未选择或修改传输所包含之信息。

[1479] For an overview of legal approaches, see also: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 18 *et seq.*, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1480] *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 253 et seq; *Lindahl,* Deduction and Justification in the Law. Role of Legal Terms and Conditions, Ratio Juris, Vol. 17, Iss. 2, 2004, page 182 et seq.

[1481] *Bayles*, Definitions in law, published in Fetzer/Shatz/Schlesinger, Definitions and Definability: Philosophical Perspectives, 1991, page 255.

[1482] Four definitions are included in Art. 1 and an additional provision was included in Art. 9, Council of Europe Convention on Cybercrime.

[1483] For more information related to legal approaches regulating the liability of access provider see below: § 6.7.4

[1484] With regard to the lawful interception of communication see below: § 6.5.9.

[1485] With regard to the liability of caching provider see below: § 6.7.5.

[1486] For more details related to different legal approaches to criminalize child pornography see below: § 6.2.8.

[1487] With regard to the criminalization of such conduct see below: § 6.2.7.

[1488] Art. 2(a) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

[1489] Art. 3(a) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

[1490] Sec. 3(3) HIPCAR Model Legislative Text on Cybercrime.

[1491] With regard to details of the criminalization see below: § 6.2.8.

[1492] For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

[1493] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1494] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

[1495] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1496] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1497] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1498] Art. 2(c) European Union Directive on combating the sexual abuse and sexual exploitation of children and child pornography, 2011/92/EU.

[1499] Art. 20(2) Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, ETS 201.

[1500] With regard to different approaches to criminalize data interference see below: § 6.2.5.

[1501] Regarding the criminalization of data espionage/illegal data acquisition see below: § 6.2.3.

[1502] Art. 1(b) Council of Europe Convention on Cybercrime, ETS 185.

[1503] Art. 1(b) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

[1504] Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

[1505] Sec. 3(5) HIPCAR Model Legislative Text on Cybercrime.

[1506] Sec.3 (7) HIPCAR Model Legislative Text.

[1507] *Stair/Reynolds/Reynolds*, Fundamentals of Information Systems, 2008, page 167; *Weik*, Computer science and communications dictionary, 2000, page 826; *Stair/Reynolds*, Principles of Information Systems, 2011, page 15.

[1508] Art. 1(a) Council of Europe Convention on Cybercrime, ETS 185.

[1509] Art. 1(a) EU Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. The Framework Decision uses the term „information“ system instead of computer system.

[1510] Art. 1 Draft ECOWAS Directive on Fighting Cyber Crime.

[1511] Sec. 3(4) HIPCAR Model Legislative Text on Cybercrime.

[1512] Regarding attacks against critical infrastructure see above: § 1.2.

[1513] Regarding the related challenges see above: § 3.2.14.

[1514] With regard to the legal response see below: § 6.5.11.

[1515] Draft African Union Convention on the Establishment of a credible Legal Framework for Cyber Security in Africa, Version 1, January 2011.

[1516] See below: § 6.2.15.

[1517] See Art. 10 (1)(a) HIPCAR Model Legislative Text on Cybercrime.

[1518] See below: § 6.2.6.

[1519] With regard to the liability of different types of provider see below: § 6.7.

[1520] Regarding the liability of search engines see below: § 6.7.10.

[1521] With regard to illegal interception, see below: § 6.2.4.

[1522] For more details related to the interference with computer data see below: § 6.2.5.

[1523] With regard to system interference see below: § 6.2.6.

[1524] See in this regard below: § 6.2.14.

[1525] See below: § 6.5.12.

[1526] Regarding the different legal approaches to seize evidence see below: § 6.5.6.

[1527] See in this regard Art. 19 (3) Council of Europe Convention on Cybercrime.

[1528] Sec. 3 Commonwealth Model Law on Computer and Computer-related Crime.

[1529] Sec. 3(17) HIPCAR Model Legislative Text on Cybercrime.

[1530] See below: § 6.5.9.

[1531] Art. 1 Council of Europe Convention on Cybercrime.

[1532] Sec. 3(18) HIPCAR Model Legislative Text on Cybercrime.

[1533] *Sieber*, Multimedia Handbook, Chapter 19, page 17. For an overview of victims of early hacking attacks, see: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history; *Joyner/Lotriont*e, Information Warfare as International Coercion: Elements of a Legal Framework, EJIL 2002, No. 5 – page 825 *et seq.*

[1534] These range from the simple proof that technical protection measures can be circumvented, to the intent to obtain data stored on the victim computer. Even political motivations have been discovered. See: *Anderson*, Hacktivism and Politically Motivated Computer Crime, 2005, available at: www.aracnet.com/~kea/Papers/Politically%20Motivated%20Computer%20Crime.pdf.

[1535] Regarding the independence of place of action and the location of the victim, see above § 3.2.7.

[1536] These can, for example, be passwords or fingerprint authorization. In addition, there are several tools available that can be used to circumvent protection measures. For an overview of potential tools, see *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, available at: www.212cafe.com/download/e-book/A.pdf.

[1537] Regarding the supportive aspects of missing technical protection measures, see *Wilson*, Computer Attacks and Cyber Terrorism, Cybercrime & Security, IIV-3, page 5. The importance of implementing effective security measures to prevent illegal access is also highlighted by the drafters of the Convention on Cybercrime. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 45.

[1538] *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 729.

[1539] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 44. "The need for protection reflects the interests of organizations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner".

[1540] With regard to data espionage, see above, § 2.5.2 and below, § 6.1.3.

[1541] With regard to data interference see above, Chapter 2.4.d and below, Chapter 6.1.3.

[1542] *Sieber*, Informationstechnologie und Strafrechtsreform, page 49 *et seq.*

[1543] For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

[1544] Art. 2 of the Convention on Cybercrime enables the Member States to keep those existing limitations that are mentioned in Art. 2, sentence 2. Regarding the possibility of limiting criminalization, see also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 40.

[1545] An example of this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a). This provision was changed in 2007. The following text presents the old version:

Section 202a – Data Espionage

(1) Whoever, without authorization, obtains data for himself or another, which was not intended for him and was specially protected against unauthorized access, shall be punished with imprisonment for not more than three years or a fine.

(2) Within the meaning of subsection (1), data shall only be those which stored or transmitted electronically or magnetically or otherwise in a not immediately perceivable manner.

[1546] This approach is not only found in national legislation, but was also recommended by Council of Europe Recommendation No. (89) 9.

[1547] For an overview of the various legal approaches in criminalizing illegal access to computer systems, see *Schjolberg*, The Legal Framework – Unauthorized Access To Computer Systems – Penal Legislation In 44 Countries, 2003, available at: www.mosstingrett.no/info/legal.html.

[1548] Regarding the system of reservations and restrictions, see *Gercke*, The Convention on Cybercrime, Computer Law Review International, 2006, 144.

[1549] *Gercke*, Cybercrime Training for Judges, 2009, page 27, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1550] With regard to software tools that are designed and used to carry out such attacks, see: *Ealy*, A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention, page 9 *et seq.*, available at: www.212cafe.com/download/e-book/A.pdf. With regard to Internet-related social engineering techniques, see the information offered by the anti-phishing working group, available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1551] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

[1552] The relevance of attacks by insiders is highlighted by the 2007 CSI Computer Crime and Security Survey. The survey notes that 5 per cent of the respondents reported that 80-100 per cent of their losses were caused by insiders. Nearly 40 per cent of all respondents reported that between 1 per cent and 40 per cent of the losses related to computer and network crimes were caused by insiders. For more details, see: 2007 CSI Computer Crime and Security Survey, page 12, available at: www.gocsi.com/.

[1553] Reservations and restrictions are two possibilities of adjusting the requirements of the Convention to the requirements of individual national legal systems.

[1554] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 46.

[1555] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1556] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1557] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self-defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1558] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47.

[1559] *Jones*, Council of Europe Convention on Cybercrime: Themes and Critiques, page 7.

[1560] See for example: World Information Technology And Services Alliance (WITSA), Statement On The Council Of Europe Draft Convention On Cybercrime, 2000, available at: www.witsa.org/papers/COEstmt.pdf. Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1561] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62 (dealing with Article 4).

[1562] *Granger*, Social Engineering Fundamentals, Part I: Hacker Tactics, Security Focus, 2001, available at: www.securityfocus.com/infocus/1527.

[1563] This is especially relevant for phishing cases. See in this context: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see below: § 2.9.4.

[1564] *Gercke*, Cybercrime Training for Judges, 2009, page 28, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1565] Article 42 – Reservations: By a written notification addressed to the Secretary-General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

[1566] This limits the criminalization of illegal access to those cases where the victim used technical protection measures to protect its computer system. Access an unprotected computer system would therefore not be considered a criminal act.

[1567] The additional mental element/motivation enables Member States to undertake a more focused approach rather than implementing a criminalization of the mere act of hacking. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 47, and Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

[1568] This enables Member States to avoid a criminalization of cases where the offender had physical access to the computer system of the victim and therefore did not need to perform an Internet-based attack.

[1569] Framework Decision on Attacks against Information Systems – 19 April 2002 – COM (2002) 173. For more details, see above: § 5.2.1.

[1570] Article 2 – Illegal access to information systems:

1. Each Member State shall take the necessary measures to ensure that the intentional access without right to the whole or any part of an information system is punishable as a criminal offence, at least for cases that are not minor.

2. Each Member State may decide that the conduct referred to in paragraph 1 is incriminated only where the offence is committed by infringing a security measure.

committed by infringing a security measure.

[1571] Model Law on Computer and Computer Related Crime, LMM(02)17, available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1572] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1573] See the explanation of the Council Framework Decision 2005/222/JHA, 1.6.

[1574] Council Framework Decision 2005/222/JHA (13).

[1575] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the United States in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cybercrime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1576] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1577] See *Sofaer/Goodman/Cuellar/Drozdova and others*. A Proposal for an International Convention on Cybercrime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1578] In this context, "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

[1579] Standalone computer systems are covered by Art. 1, paragraph 3, of the Draft Convention because they "control programs". This does not require a network connection.

[1580] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1581] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1582] The Explanatory Report points out that the provision intends to criminalize violations of the right of privacy of data communication. See the Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1583] See below: § 6.1.4.

[1584] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

[1585] One key indication of the limitation of application is the fact that the Explanatory Report compares the solution in Art. 3 to traditional violations of the privacy of communication beyond the Internet, which do not cover any form of data espionage. *"The offence represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons. The right to privacy of correspondence is enshrined in Article 8 of the European Convention on Human Rights."* See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1586] See in this context especially a recent case from Hong Kong, People's Republic of China. See above: § 2.5.2.

[1587] ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1588] Regarding the challenges related to the use of encryption technology by offenders, see above: § 3.2.14; *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; *Zanini/Edwards*, The Networking of Terror in the Information Age, in *Arquilla/Ronfeldt*, Networks and Netwars: The Future of Terror, Crime, and Militancy, page 37, available at: http://192.5.14.110/pubs/monograph_reports/MR1382/MR1382.ch2.pdf; *Flamm*, Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography, available at: www.terrorismcentral.com/Library/Teasers/Flamm.html. Regarding the underlying technology, see: *Singh*, The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

[1589] One of the consequences related to this aspect is the fact that limitation of the criminalization of illegal access to those cases where the victim of the attack secured the target computer system with technical protection measures could limit the application of such a provision, insofar as a large number of users do not have sufficient knowledge about the implementation of technical protection measures.

[1590] Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3489 (1996). See in this context: *Chamblee*, Validity, Construction, and Application of Title I of Economic Espionage Act of 1996 (18 U.S.C.A. §§ 1831 *et seq.*), 177 A.L.R. Fed. 609 (2002); *Fischer*, An Analysis of the Economic Espionage Act of 1996, 25 Seton Hall Legis. J. 239 (2001).

[1591] *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 986, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

[1592] For details, see: US CCIPS, Prosecuting Intellectual Property Crimes, 3rd Edition, 2006, page 138 *et seq.* available at: www.justice.gov/criminal/cybercrime/ipmanual/04ipma.pdf.

[1593] *Loundy*, Computer Crime, Information Warfare, and Economic Espionage, 2009, page 55 *et seq.*; *Krotosi,* Identifying and Using Evidence Early To Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, Economic Espionage and Trade Secrets, 2009, Vol. 75, No. 5, page 41 *et seq.* available at: www.justice.gov/usao/eousa/foia_reading_room/usab5705.pdf.

[1594] *Decker*, Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime, Southern California Law Review, 2008, Vol. 81, page 988, available at: http://weblaw.usc.edu/why/students/orgs/lawreview/documents/Decker_Charlotte_81_5.pdf.

[1595] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1596] The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1597] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010. The document is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1598] This provision has recently been modified and now even criminalizes illegal access to data. The previous version of the provision has been used here, because it is better suited for demonstrating the dogmatic structure.

[1599] See *Hoyer* in SK-StGB, Sec. 202a, Nr. 3.

[1600] A similar approach of limiting criminalization to cases where the victim did not take preventive measures can be found in Art. 2, sentence 2, Convention on Cybercrime: *A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.* For more information, see above: § 6.1.1.

[1601] This provision is therefore an example for of a legislative approach that should not substitute for, but rather complement, self-protection measures.

[1602] See in this context for example a recent case in Hong Kong: *Watts,* Film star sex scandal causes internet storm in China, The Guardian, 12.02.2008, available at: www.guardian.co.uk/world/2008/feb/12/china.internet; *Tadros*, Stolen photos from laptop tell a tawdry tale, The Sydney Morning Herald, 14.02.2008, available at: www.smh.com.au/news/web/stolen-photos-from-laptop-tell-a-tawdry-tale/2008/02/14/1202760468956.html; *Pomfret*, Hong Kong's Edision
Chen quits after sex scandal, Reuters, 21.02.2008, available at: www.reuters.com/article/entertainmentNews/idUSHKG36060820080221?feedType=RSS&feedName=entertainmentNews; *Cheng*, Edision Chen is a celebrity, Taipei Times, 24.02.2008, available at: www.taipeitimes.com/News/editorials/archives/2008/02/24/2003402707.

[1603] The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1604] With regard to "phishing", see above: § 2.9.4 and below: § 6.1.15 and as well: *Jakobsson*, The Human Factor in Phishing, available at: www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, Computer und Recht 2005, page 606. The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, Phishing, Computer und Recht, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing, see above: § 2.9.4.

[1605] Regarding the risks related to the use of wireless networks, see above: § 3.2.3. Regarding the difficulties in cybercrime investigations that include wireless networks, see *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors, Australian Institute of Criminology, 2006, available at: www.aic.gov.au/publications/tandi2/tandi329t.html.

[1606] Regarding the architecture of the Internet, see: *Tanebaum*, Computer Networks; *Comer*, Internetworking with TCP/IP – Principles, Protocols and Architecture.

[1607] Regarding the underlying technology and the security related issues, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx. With regard to the advantages of wireless networks for the development of ICT infrastructure in developing countries, see: The Wireless Internet Opportunity for Developing Countries, 2003, available at: www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

[1608] The computer magazine ct reported in 2004 that field tests proved that more than 50 per cent of 1 000 wireless computer networks that were tested in Germany were not protected. See: www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/48182.

[1609] Regarding the impact of encryption of wireless communication, see: *Sadowsky/Dempsey/Greenberg/Mack/Schwartz*, Information Technology Security Handbook, page 60, available at: www.infodev.org/en/Document.18.aspx.

[1610] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 31, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1611] Regarding identity theft, see above: § 2.8.3 and below: § 6.1.16 and also: Javelin Strategy & Research 2006 Identity Fraud Survey, Consumer Report, available at: www.javelinstrategy.com/products/99DEBA/27/delivery.pdf. For further information on other surveys, see *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, page 9, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Lee*, Identity Theft Complaints Double in '02, New York Times, Jan. 22, 2003; *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_cooperation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf. For an approach to divide between four phases, see: *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 21 *et seq.*, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[1612] In the United States, the SSN was created to keep an accurate record of earnings. Contrary to its original intentions, the SSN is today widely used for identification purposes. Regarding offences related to social-security numbers, see: *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm; *Sobel*, The Demeaning of Identity and personhood in National Identification Systems, Harvard Journal of Law & Technology, Vol. 15, Nr. 2, 2002, page 350.

[1613] See: *Hopkins*, Cybercrime Convention: A Positive Beginning to a Long Road Ahead, Journal of High Technology Law, 2003, Vol. II, No. 1, page 112.

[1614] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

[1615] The Explanatory Report describes the technical means more in detail: "Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes. The requirement of using technical means is a restrictive qualification to avoid over-criminalization." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

[1616] Within this context, only interceptions made by technical means are covered by the provision – Article 3 does not cover acts of "social engineering".

[1617] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 730.

[1618] *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf

[1619] See above: § 6.1.3.

[1620] "The communication in the form of transmission of computer data can take place inside a single computer system (flowing from CPU to screen or printer, for example) between two computer systems belonging to the same person, two computers communicating with one another or a computer and a person (e.g. through the keyboard)." Explanatory Report to the Council of Europe Convention on Cybercrime, No. 55.

[1621] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 53.

[1622] Covered by Article 3 is the interception of electronic emissions that are produced during the use of a computer. Regarding this issue, see Explanatory Report, No. 57: *"The creation of an offence in relation to "electromagnetic*

emissions" will ensure a more comprehensive scope. Electromagnetic emissions may be emitted by a computer during its operation. Such emissions are not considered as "data" according to the definition provided in Article 1. However, data can be reconstructed from such emissions. Therefore, the interception of data from electromagnetic emissions from a computer system is included as an offence under this provision", Explanatory Report to the Council of Europe Convention on Cybercrime, No. 57.

1623 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 51.

1624 *Gercke*, Cybercrime Training for Judges, 2009, page 29, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1625 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 54.

1626 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1627 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1628 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1629 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1630 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1631 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1632 Cookies are data sent by a server to a browser and then sent back each time the browser is used to access the server. Cookies are used for authentication, tracking and keeping user information. Regarding the functions of cookies and the controversial legal discussion, see: *Kesan/Shah*, Deconstruction Code, Yale Journal of Law & Technology, 2003-2004, Vol. 6, page 277 *et seq.*, available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=597543.

1633 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 58.

1634 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1635 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1636 Model Law on Computer and Computer Related Crime" LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1637 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf.
For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1638] The difficulty with offences against the integrity of data is that identification of these violations is often difficult to prove. Therefore, the Expert Group which drafted the Convention on Cybercrime identified the possibility of prosecuting violations regarding data interference by means of criminal law as a necessary strategic element in the fight against cybercrime. Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

[1639] The 2007 Computer Economics Malware Report focuses on computer crime and analyses the impact of malware on the worldwide economy by summing up the estimated costs caused by attacks. It identified peaks in 2000 (USD 17.1 billion) and 2004 (USD 17.5 billion). For more information, see: 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and Other malicious Code. A summary of the report is available at: www.computereconomics.com/article.cfm?id=1225.

[1640] A number of computer fraud scams are including the manipulation of data – e.g. the manipulation of bank-account files, transfer records or data on smart cards. Regarding computer related fraud scams, see above: § 2.8.1 and below: § 6.1.17.

[1641] Regarding the problems related to these gaps, see for example the LOVEBUG case, where a designer of a computer worm could not be prosecuted due to the lack of criminal law provisions related to data interference. See above: § 2.5.4 and: CNN, Love Bug virus raises spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10, available at: http://media.hoover.org/documents/0817999825_1.pdf; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: http://www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1642] A similar approach to Art. 4 of the Convention on Cybercrime is found in the EU Framework Decision on Attacks against Information Systems: Article 4 – Illegal data interference: "Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor".

[1643] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 60.

[1644] As pointed out in the Explanatory Report, the two terms overlap. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1645] Regarding the more conventional ways to delete files using Windows XP, see the information provided by Microsoft, available at: www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx.

[1646] Regarding the consequences for forensic investigations, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq.*, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1647] See *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/05hb003.pdf.

[1648] The fact that the Explanatory Report mentions that the files are unrecognizable after the process does not give any further indication with regard to the interpretation of the term. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1649] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1650] A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf. In 2000 a number of well-known US e-commerce businesses were targeted by DoS attacks. A full list is provided by *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and

Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1651 With regard to the criminalization of DoS attacks, see also below: § 6.1.6.

1652 In addition, criminalization of DoS attacks is provided by Art. 5 of the Convention on Cybercrime. See below: § 6.1.6.

1653 Apart from the input of malicious codes (e.g. viruses and trojan horses), it is likely that the provision could cover unauthorized corrections of faulty information as well.

1654 *Gercke*, Cybercrime Training for Judges, 2009, page 32, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Regarding the different recognized functions of malicious software, see above: § 2.5.4. Regarding the economic impact of malicious software attacks, see above: § 2.5.4.

1655 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1656 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1657 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report states: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized"*. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1658 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62: "The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g., encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right." Regarding the liability of Remailer, see: *Du Pont*, The time has come for limited liability for operators of true Anonymity Remails in Cyberspace: An Examination of the possibilities and perils, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

1659 For further information, see *du Pont*, The Time Has Come For Limited Liability For Operators Of True Anonymity Remailers In Cyberspace: An Examination Of The Possibilities And Perils, Journal Of Technology Law & Policy, Vol. 6, Issue 2, page 176 *et seq.*, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/duPont.pdf.

1660 With regard to the possible difficulties to identify offenders who have made use of anonymous or encrypted information, the Convention leaves the criminalization of anonymous communications open to the parties to decide on – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 62.

1661 Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems.

1662 For further information, see: *Gercke*, The EU Framework Decision on Attacks against Information Systems, Computer und Recht 2005, page 468 *et seq.*

1663 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1664 See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

1665 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1666 Sec. 5 (Illegal access), Sec. 8 (Illegal interception) and Sec. 10 (Child pornography).

1667 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cybercrime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1668 ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 33, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

1669 A denial-of-service (DoS) attack aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see above: § 2.5.4 and US-CERT, Understanding Denial-of-Service Attacks, available at: www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

1670 For an overview of successful attacks against famous Internet companies, see: *Moore/Voelker/Savage*, Inferring Internet Denial-of-Service Activities, page 1, available at: www.caida.org/papers/2001/BackScatter/usenixsecurity01.pdf; CNN News, One year after DoS attacks, vulnerabilities remain, at: http://edition.cnn.com/2001/TECH/internet/02/08/ddos.anniversary.idg/index.html. *Yurcik*, Information Warfare Survivability: Is the Best Defense a Good Offence?, page 4, available at: www.projects.ncassr.org/hackback/ethics00.pdf. For more information, see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 *et seq.*; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000, available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security, Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3, available at: www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

1671 Regarding the possible financial consequences of lack of availability of Internet services due to attack, see: Campbell/Gordon/Loeb/Zhou, The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market, Journal of Computer Security, Vol. 11, pages 431-448.

1672 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 34, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Regarding cyberterrorism, see above § 2.9.1 and *Lewis*, The Internet and Terrorism, available at: www.csis.org/media/csis/pubs/050401_internetandterrorism.pdf; *Lewis*, Cyberterrorism and Cybersecurity, available at: www.csis.org/media/csis/pubs/020106_cyberterror_cybersecurity.pdf; *Denning*, Activism, hacktivism, and cyberterrorism: the Internet as a tool for influencing foreign policy, in *Arquilla/Ronfeld*t, Networks & Netwars: The Future of Terror, Crime, and Militancy, page 239 *et seq.*, available at: www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf; *Embar-Seddon*, Cyberterrorism, Are We Under Siege?, American Behavioral Scientist, Vol. 45 page 1033 *et seq.*; United States Department of State, Pattern of Global Terrorism, 2000, in: *Prados*, America Confronts Terrorism, 2002, 111 *et seq.*; *Lake*, 6 Nightmares, 2000, page 33 et *seq.*; *Gordon*, Cyberterrorism, available at: www.symantec.com/avcenter/reference/cyberterrorism.pdf; United States National Research Council, Information Technology for Counterterrorism: Immediate Actions and Future Possibilities, 2003, page 11 *et seq.* OSCE/ODIHR Comments on legislative treatment of "cyberterror" in domestic law of individual states, 2007, available at: www.legislationline.org/upload/lawreviews/93/60/7b15d8093cbebb505ecc3b4ef976.pdf; *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, pages 221-249.

1673 The protected legal interest is the interest of operators as well as users of computer or communication systems being able to have them function properly. See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 65.

[1674] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

[1675] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1676] The Explanatory Report gives examples for implementation of restrictive criteria for serious hindering: "Each Party shall determine for itself what criteria must be fulfilled in order for the hindering to be considered "serious." For example, a Party may require a minimum amount of damage to be caused in order for the hindering to be considered serious. The drafters considered as "serious" the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems (e.g. by means of programs that generate "denial-of-service" attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge quantities of electronic mail to a recipient in order to block the communications functions of the system)" – See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 67.

[1677] *Gercke*, Cybercrime Training for Judges, 2009, page 35, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf. Although the connotation of "serious" does limit the applicability, it is likely that even serious delays to operations resulting from attacks against a computer system can be covered by the provision.

[1678] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 66.

[1679] Examples are the use of networks (wireless or cable networks), bluetooth or infrared connection.

[1680] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61. Regarding the fact that the definition does not distinguish between the different ways how information can be deleted, see above: § 6.1.15. Regarding the impact of the different ways of deleting data on computer forensics, see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 *et seq*., available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[1681] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1682] Apart from the input of malicious codes (e.g. viruses and trojan horses), it is therefore likely that the provision could cover unauthorized corrections of faulty information as well. .

[1683] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

[1684] "Spam" describes the process of sending out unsolicited bulk messages. For a more precise definition, see: ITU Survey on Anti-Spam legislation worldwide 2005, page 5, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf. For more information, see above: § 2.5.g.

[1685] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf

[1686] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1687] Regarding legal approaches in the fight against spam, see above: § 6.1.l3.

[1688] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69.

[1689] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1690] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1691] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: *"A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression "without right" derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and*

common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalized". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1692] See for example: World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1693] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 68: "The hindering must be "without right". Common activities inherent in the design of networks, or common operational or commercial practices are with right. These include, for example, the testing of the security of a computer system, or its protection, authorized by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalized by this article, even if it causes serious hindering."

[1694] Framework Decision on attacks against information systems – 19 April 2002 – COM (2002) 173.

[1695] Article 3 – Illegal system interference: "Each Member State shall take the necessary measures to ensure that the intentional serious hindering or interruption of the functioning of an information system by inputting, transmitting, damaging, deleting, deteriorating, altering, suppressing or rendering inaccessible computer data is punishable as a criminal offence when committed without right, at least for cases which are not minor".

[1696] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cybercrime: National Legislation as a prerequisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1697] See the explanation of the EU Directive 2013/40/EU on attacks against information systems.

[1698] Draft Convention on Cybercrime (Draft No. 19), European Committee On Crime Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), PC-CY (2000), 19, available at: www.iwar.org.uk/law/resources/eu/cybercrime.htm.

[1699] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/ documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1700] For an overview on hate speech legislation, see for example: the database provided at: www.legislationline.org. For an overview on other cybercrime-related legislation, see: the database provided at: www.cybercrimelaw.net.

[1701] Regarding the challenges of international investigation, see above: § 3.2.4 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1702] For details, see: *Wolters/Horn*, SK-StGB, Sec. 184, Nr. 2.

[1703] *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 5.

[1704] Regarding the influence of pornography on minors, see: *Mitchell/Finkelhor/Wolak*, The exposure of youth to unwanted sexual material on the Internet – A National Survey of Risk, Impact, and Prevention, Youth & Society, Vol. 34, 2003, page 330 *et seq.*, available at: www.unh.edu/ccrc/pdf/Exposure_risk.pdf; *Brown*, Mass media influence on sexuality, Journal of Sex Research, February 2002, available at: http://findarticles.com/p/articles/mi_m2372/is_1_39/ai_87080439.

[1705] See Section 11 Subparagraph 3 Penal Code: "Audio and visual recording media, data storage media, illustrations and other images shall be the equivalent of writings in those provisions which refer to this subsection".

[1706] *Hoernle* in Muenchener Kommentar StGB, Sec. 184, No. 28.

[1707] The draft law was not in force by the time this publication was finalized.

[1708] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1709] Regarding the challenges of international investigation, see above: § 3.2.4. See also: *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1710] *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279; *Cox*, Litigating Child Pornography and Obscenity Cases, Journal of Technology Law and Policy, Vol. 4, Issue 2, 1999, available at: http://grove.ufl.edu/~techlaw/vol4/issue2/cox.html#enIIB.

[1711] Regarding methods of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 *et seq.*, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729. Regarding the challenges related to anonymous communication, see above: § 3.2.14.

[1712] It has been reported that some websites containing child pornography register up to a million hits per day. For more information, see: *Jenkins*, Beyond Tolerance: Child Pornography on the Internet, 2001, New York University Press; *Wortley/Smallbone*, Child Pornography on the Internet, page 12, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1713] Regarding the challenges related to investigations involving anonymous communication technology, see above: § 3.2.l.

[1714] Regarding the possibilities of tracing offenders of computer-related crimes, see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[1715] *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 68.

[1716] *Liu*, Ashcroft, Virtual Child Pornography and First Amendment Jurisprudence, UC Davis Journal of Juvenile Law & Policy, 2007, Vol. 11, page 6, available at: http://jjlp.law.ucdavis.edu/archives/vol-11-no-1/07%20Liu%2011.1.pdf.

[1717] *Levesque*, Sexual Abuse of Children: A Human Rights Perspective, 1999, page 69.

[1718] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

[1719] *Akdeniz* in *Edwards/Waelde*, Law and the Internet: Regulating Cyberspace; *Williams* in *Miller*, Encyclopaedia of Criminology, page 7. Regarding the extent of criminalization, see: Child Pornography: Model Legislation & Global Review, 2006, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf. Regarding the discussion about the criminalization of child pornography and freedom of speech in the United States, see: *Burke*, Thinking Outside the Box: Child Pornography, Obscenity and the Constitution, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue3/v8i3_a11-Burke.pdf; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws in terms of the criminalization of child pornography.

[1720] Regarding differences in legislation, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 26, available at: www.cops.usdoj.gov/mime/open.pdf?Item=1729.

[1721] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 91.

[1722] *Walden*, Computer Crimes and Digital Investigations, 2006, page 144.

[1723] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 94.

[1724] Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse, ETS 201.

[1725] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 135.

[1726] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1727] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 95.

[1728] Regarding criminalization of the possession of child pornography in Australia, see: *Krone*, Does thinking make it so? Defining online child pornography possession offences, in "Trends & Issues in Crime and Criminal Justice", No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet. This article compares various national laws regarding the criminalization of child pornography.

[1729] See: Child Pornography: Model Legislation & Global Review, 2006, page 2, available at: www.icmec.org/en_X1/pdf/ModelLegislationFINAL.pdf.

[1730] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 98.

[1731] *Gercke*, Cybercrime Training for Judges, 2009, page 45, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf

[1732] Based on the National Juvenile Online Victimization Study, only 3 per cent of arrested Internet-related child-pornography possessors had morphed pictures. *Wolak/ Finkelhor/ Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[1733] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 102.

[1734] *Wortley/Smallbone*, Child Pornography on the Internet, Problem-oriented Guides for Police, No. 31, page 7, available at: www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf.

[1735] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1736] Available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1737] Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly Resolution 44/25 of 20 November 1989, entry into force 2 September 1990, in accordance with Article 49. Article 1. For the purposes of the present Convention, a child means every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier.

[1738] One example is the current German Penal Code. The term "child" is defined by law in Section 176 to which the provision related to child pornography refers: Section 176: "Whoever commits sexual acts on a person under fourteen years of age (a child) ...".

[1739] Council Framework Decision on combating the sexual exploitation of children and child pornography, 2004/68/JHA, available at: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf.

[1740] Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS No. 201, available at: http://conventions.coe.int.

[1741] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 104.

[1742] For an overview of the legal age of consent and child pornography in selected countries, see: Prevention of Child Pornography, LC Paper No. CB(2)299/02-03(03), available at: www.legco.gov.hk/yr01-02/english/bc/bc57/papers/bc571108cb2-299-3e.pdf.

[1743] See in this regard: R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R 45, available at: www.canlii.org/en/ca/scc/doc/2001/2001scc2/2001scc2.html.

[1744] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1745] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1746] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1747] *Gercke*, Cybercrime Training for Judges, 2009, page 46, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_pdf.

[1748] Regarding the challenges related to the use of encryption technology, see above: § 3.2.14. One survey on child pornography suggested that only 6 per cent of arrested child-pornography possessors used encryption technology. See: *Wolak/Finkelhor/Mitchell*, Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study, 2005, page 9, available at: www.missingkids.com/en_US/publications/NC144.pdf.

[1749] See Explanatory Report to the Convention on the Protection of Children, No. 140.

[1750] The download is in general necessary to enable the display of the information on the website. Depending on the configuration of the browser, the information can be downloaded to cache and temp files or is just stored in the RAM memory of the computer. Regarding the forensic aspects of this download, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 180, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[1751] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1752] Official Notes:

NOTE: The laws respecting pornography vary considerably throughout the Commonwealth. For this reason, the prohibition in the model law is limited to child pornography, which is generally the subject of an absolute prohibition in all member countries. However a country may wish to extend the application of this prohibition to other forms of pornography, as the concept may be defined under domestic law.

NOTE: The pecuniary penalty will apply to a corporation but the amount of the fine may be insufficient. If it is desired to provide a greater penalty for corporations, the last few lines of subsection (1) could read: "commits an offence punishable, on conviction:

(a) in the case of an individual, by a fine not exceeding [amount] or imprisonment for a period not exceeding [period]; or

(b) in the case of a corporation, by a fine not exceeding [a greater amount].

[1753] Official Note:

NOTE: Countries may wish to reduce or expand upon the available defences set out in paragraph 2, depending on the particular context within the jurisdiction. However, care should be taken to keep the defences to a minimum and to avoid overly broad language that could be used to justify offences in unacceptable factual situations.

[1754] See the preface to the Optional Protocol.

[1755] See Art. 2.

[1756] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf.
For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1757] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1758] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1759] See in this regard: *Powell*, Paedophiles, Child Abuse and the Internet, 2007; *Eneman/Gillespie/Stahl*, Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case, AISeL, 2010, available at: www.cse.dmu.ac.uk/~bstahl/index_html_files/2010_grooming_ICIS.pdf.

[1760] See: Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

[1761] Council of Europe – Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[1762] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 155.

[1763] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 157.

[1764] Explanatory Report to the Council of Europe Convention on the Protection of Children, No. 159.

[1765] International Mechanisms for Promoting Freedom of Expression, Joint Declaration, Challenges to Freedom of Expression in the New Century, by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2001.

[1766] For an overview of hate speech legislation, see the database provided at: www.legislationline.org.

[1767] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1768] Regarding the criminalization of hate speech in Europe, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 781 *et seq.* available at: http://law.wlu.edu/ deptimages/Law%20Review/62-2VanBlarcum.pdf. Regarding the situation in Australia, see: *Gelber/Stone*, Hate Speech and Freedom of Speech in Australia, 2007.

[1769] Vienna Summit Declaration, 1993, available at: www.coe.int/t/dghl/monitoring/ecri/archives/other_texts/2-vienna/plan_of_action/plan_of_action_vienna_summit_EN.asp.

[1770] Recommendation No. 1275 on the fight against racism, xenophobia, anti-Semitism and intolerance.

[1771] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4: "The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention."

[1772] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: http://conventions.coe.int.

[1773] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*; Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1774] Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

[1775] Regarding the list of states that signed the Additional Protocol, see above: § 5.2.1.

[1776] Regarding the difficulties related to the jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

[1777] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at: www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1778] Regarding the challenges of international investigation, see above: § 3.2.5 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1779] Regarding possible reservations, see: *Blarcum*, Internet Hate Speech, The European Framework and the Emerging American Haven, Washington and Lee Law Review, 2007, page 792.

[1780] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1781] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1782] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 28.

[1783] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 29.

[1784] Regarding the definition of "distributing" and "making available", see § 6.1.8 above.

[1785] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 34.

[1786] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1787] Explanatory Report to the First Addition Protocol to the Convention on Cybercrime, No. 36.

[1788] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1789] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1790] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1791] Regarding legislation on blasphemy, as well as other religious offences, see: Preliminary Report On The National Legislation In Europe Concerning Blasphemy, Religious Insults And Inciting Religious Hatred, 2007, available at: www.venice.coe.int/docs/2007/CDL-AD(2007)006-e.pdf.

[1792] International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2006.

[1793] See above: § 6.1.9, as well as Explanatory Report to the First Additional Protocol to the Council of Europe Convention on Cybercrime, No. 4.

[1794] The draft law was not in force at the time this publication was finalized.

[1795] Prevention of Electronic Crimes Ordinance 2007, available at: www.upesh.edu.pk/net-infos/cyber-act08.pdf.

[1796] Prevention of Electronic Crimes Ordinance, 2007, published in the Gazette of Pakistan, Extraordinary, Part-I, dated 31 December 2007, available at: www.na.gov.pk/ordinances/ord2008/elect_crimes_10042008.pdf.

[1797] Regarding the principle of freedom of speech, see: *Tedford/Herbeck/Haiman*, Freedom of Speech in the United States, 2005; *Barendt*, Freedom of Speech, 2007; *Baker*, Human Liberty and Freedom of Speech; *Emord*, Freedom, Technology and the First Amendment, 1991. Regarding the importance of the principle with regard to electronic surveillance, see: *Woo/So*, The case for Magic Lantern: September 11 Highlights the need for increasing surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 530 *et seq.*; *Vhesterman*, Freedom of Speech in Australian Law; A Delicate Plant, 2000; *Volokh*, Freedom of Speech, Religious Harassment Law, and Religious Accommodation Law, Loyola University Chicago Law Journal, Vol. 33, 2001, page 57 *et seq.*, available at: www.law.ucla.edu/volokh/harass/religion.pdf; *Cohen*, Freedom of Speech and Press: Exceptions to the First Amendment, CRS Report for Congress 95-815, 2007, available at: www.fas.org/sgp/crs/misc/95-815.pdf.

[1798] Regarding the difficulties related to jurisdiction and the principle of freedom of expression, see also: Report on Legal Instruments to Combat Racism on the Internet, Computer Law Review International (2000), 27, available at: www.coe.int/t/e/human_rights/ecri/1-EComputerLawReviewInternational/3-General_themes/3-Legal_Research/2-Combat_racism_on_Internet/ComputerLawReviewInternational(2000)27.pdf.

[1799] Dual criminality exists if the offence is a crime under both the requested and requesting party's laws. The difficulties the dual criminality principle can cause within international investigations are a current issue in a number of international conventions and treaties. Examples include Art. 2 of the EU Framework Decision of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (2002/584/JHA). Regarding the dual criminality principle in international investigations, see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269, available at www.uncjin.org/Documents/EighthCongress.html; *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5, available at: www.itu.int/osg/spu/cybersecurity/presentations/session12_schjolberg.pdf.

[1800] Regarding the challenges of international investigation, see above: § 3.2.6 and *Gercke*, The Slow Wake of A Global Approach Against Cybercrime, Computer Law Review International 2006, 142. For examples, see *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension, in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 16, available at: http://media.hoover.org/documents/0817999825_1.pdf.

[1801] The 2005 e-gaming data report estimates total Internet gambling revenues as USD 3.8 billion in 2001 and USD 8.2 billion in 2004. For more details, see: www.cca-i.com/Primary%20Navigation/Online%20Data%20Store/internet_gambling_data.htm. Regarding the number of licensed Internet websites related to Internet gambling in selected countries, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 52, available at: www.gao.gov/new.items/d0389.pdf. Regarding the total numbers of Internet gambling websites, see: *Morse*, Extraterritorial Internet Gambling: Legal Challenges and Policy Opinion, page 7, available at: http://law.creighton.edu/pdf/4/morsepublication2.pdf.

[1802] For an overview of different national Internet gambling legislation, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 45 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

[1803] Regarding the situation in the People's Republic of China, see for example: Online Gambling challenges China's gambling ban, available at: www.chinanews.cn/news/2004/2005-03-18/2629.shtml.

[1804] Regarding addiction, see: *Shaffer*, Internet Gambling & Addiction, 2004, available at: www.ncpgambling.org/media/pdf/eapa_flyer.pdf; *Griffiths/Wood*, Lottery Gambling and Addiction; An Overview of European Research, available at: www.european-lotteries.org/data/info_130/Wood.pdf; *Jonsson/Andren/Nilsson/Svensson/Munck/Kindstedt/Rönnberg*, Gambling addiction in Sweden – the characteristics of problem gamblers, available at: www.fhi.se/shop/material_pdf/gamblingaddictioninsweden.pdf; National Council on Problem Gambling, Problem Gambling Resource & Fact Sheet, www.ncpgambling.org/media/pdf/eapa_flyer.pdf.

[1805] See the decision from the German Federal Court of Justice (BGH), published in BGHST 11, page 209.

[1806] See *Thumm*, Strafbarkeit des Anbietens von Internetglueckksspielen gemaess § 284 StGB, 2004.

[1807] Examples of equipment in Internet-related cases could include servers, as well as Internet connections. Internet service providers which do not know that their services are abused by offenders to run illegal gambling operations are thus not responsible, as they may lack intention.

[1808] For details, see: *Hoyer*, SK-StGB, Sec. 284, Nr. 18. As mentioned previously, criminalization is limited to those cases where the offender is intentionally making the equipment available.

[1809] This is especially relevant with regard to the location of the server.

[1810] Avoiding the creation of safe havens is a major intention of harmonization processes. The issue of safe havens has been addressed by a number of international organizations. UN General Assembly Resolution 55/63 states that: "*States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies*". The full text of the resolution is available at: www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "*There must be no safe havens for those who abuse information technologies*".

[1811] With regard to the principle of sovereignty, changing the location of a server can have a great impact on the ability of law-enforcement agencies to carry out an investigation. National Sovereignty is a fundamental principle in International Law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[1812] Regarding the challenges related to the international dimension and the independence of place of action and the location of the crime scene, see above: §§ 3.2.6 and 3.2.7.

[1813] For details, see: *Hoyer*, SK-StGB, Sec. 285, Nr. 1.

[1814] Regarding the vulnerability of Internet gambling to money laundering, see: Internet Gambling – An overview of the Issue, GAO-03-89, page 5, 34 *et seq.*, available at: www.gao.gov/new.items/d0389.pdf.

[1815] Regarding other recent approaches in the United States, see: *Doyle*, Internet Gambling: A Sketch of Legislative Proposals in the 108th Congress, CRS Report for Congress No. RS21487, 2003, available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-4047: *Doyle*, Internet Gambling: Two Approaches in the 109th Congress, CRS Report for Congress No. RS22418, 2006, available at: www.ipmall.info/hosted_resources/crs/RS22418-061115.pdf.

[1816] For an overview of the law, see: *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm; *Shaker*, America's Bad Bet: How the Unlawful Internet Gambling Enforcement act of 2006 will hurt the house, Fordham Journal of Corporate & Financial Law, Vol. XII, page 1183 *et seq.*, available at: http://law.fordham.edu/publications/articles/600flspub8956.pdf.

[1817] *Landes*, Layovers And Cargo Ships: The Prohibition Of Internet Gambling And A Proposed System Of Regulation, available at: www.law.nyu.edu/JOURNALS/LAWREVIEW/issues/vol82/no3/NYU306.pdf; *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm.

[1818] *Rose*, Gambling and the Law: The Unlawful Internet Gambling Enforcement Act of 2006 Analyzed, 2006, available at: www.gamblingandthelaw.com/columns/2006_act.htm

[1819] Based on Sec. 5366, criminalization is limited to the acceptance of financial instruments for unlawful Internet gambling.

[1820] See: EU opens investigation into US Internet gambling laws, EU Commission press release, 10.03.2008, available at: http://ec.europa.eu/trade/issues/respectrules/tbr/pr100308_en.htm; *Hansen*, EU investigates DOJ internet gambling tactics, The Register, 11.03.2008, available at: www.theregister.co.uk/2008/03/11/eu_us_internet_gambling_probe/.

[1821] General Agreement on Trade in Services (GATS) – with regard to the United States Unlawful Internet Gambling Enforcement Act especially Articles XVI (dealing with Market Access) and XVII (dealing with National Treatment) could be relevant.

[1822] See above: § 3.2.l.

[1823] See above: § 3.2.2.

[1824] See, for example: Freedom of Expression, Free Media and Information, Statement of Mr McNamara, US delegation to OSCE, October 2003, available at: http://osce.usmission.gov/archive/2003/10/FREEDOM_OF_EXPRESSION.pdf; *Lisby*, No Place in the Law: Criminal Libel in American Jurisprudence, 2004, available at: http://www2.gsu.edu/~jougcl/projects/40anniversary/criminallibel.pdf. Regarding the development of the offence, see: *Walker*, Reforming the Crime of Libel, New York Law School Law Review, Vol. 50, 2005/2006, page 169, available at: www.nyls.edu/pdfs/NLRVol50-106.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf; Defining Defamation, Principles on Freedom of Expression and Protection of Reputation, 2000, available at: www.article19.org/pdfs/standards/definingdefamation.pdf; *Reynolds*, Libel in the Blogosphere: Some Preliminary Thoughts, Washington University Law Review, 2006, page 1157 *et seq.*, available at: http://ssrn.com/abstract=898013; *Solove*, A Tale of Two Bloggers: Free Speech and Privacy in the Blogosphere, Washington University Law Review, Vol. 84, 2006, page 1195 *et seq.*, available at http://ssrn.com/abstract=901120; *Malloy*, Anonymous Bloggers And Defamation: Balancing Interests On The Internet, Washington University Law Review, Vol. 84, 2006, page 1187 *et seq.*, available at: http://law.wustl.edu/WULR/84-5/malloy.pdf.

[1825] See, for example, the Joint Declaration by the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 10 December 2002. For more information, see: www.osce.org/documents/rfm/2004/10/14893_en.pdf. See in addition the statement of the representative on Freedom of the Media, Mr Haraszti, at the fourth Winder Meeting of the OSCE Parliamentary Assembly on 25 February 2005.

[1826] Regarding various regional approaches to criminalization of defamation, see: *Greene* (eds), It's a Crime: How Insult Laws Stifle Press Freedom, 2006, available at: www.wpfc.org/site/docs/pdf/It's_A_Crime.pdf; *Kirtley*, Criminal Defamation: An Instrument of Destruction, 2003, available at: www.silha.umn.edu/oscepapercriminaldefamation.pdf.

[1827] For more details, see: the British Crime Survey 2006/2007 published in 2007, available at: www.homeoffice.gov.uk/rds/pdfs07/hosb1107.pdf.

[1828] See: Crime Statistic Germany (Polizeiliche Kriminalstatistik), 2006, available at: www.bka.de/pks/pks2006/download/pks-jb_2006_bka.pdf.

[1829] The full version of the Criminal Defamation Amendment Bill 2002 is available at: http://www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02_P.pdf. For more information about the Criminal Defamation Amendment Bill 2002, see the Explanatory Notes, available at: www.legislation.qld.gov.au/Bills/50PDF/2002/CrimDefAB02Exp_P.pdf.

[1830] The full text of the Criminal Code of Queensland, Australia is available at: www.legislation.qld.gov.au/LEGISLTN/CURRENT/C/CriminCode.pdf.

[1831] The provider Postini published a report in 2007 that identifies up to 75 per cent spam e-mail, see: www.postini.com/stats/. The Spam-Filter-Review identifies up to 40 per cent spam e-mails, see: http://spam-filter-review.toptenreviews.com/spam-statistics.html. The Messaging Anti-Abuse Working Group reported in 2005 that up to 85 per cent of all e-mails are spam. See: http://www.maawg.org/about/FINAL_4Q2005_Metrics_Report.pdf.

[1832] For more information on the phenomenon, see above: § 2.6.7. For a precise definition, see: ITU Survey on Anti-Spam Legislation Worldwide 2005, page 5, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1833] Regarding the development of spam e-mails, see: *Sunner*, Security Landscape Update 2007, page 3, available at: www.itu.int/osg/spu/cybersecurity/pgc/2007/events/presentations/session2-sunner-C5-meeting-14-may-2007.pdf

[1834] See ITU Survey on Anti-Spam Legislation Worldwide, 2005, available at: http://www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1835] Regarding the availability of filter technology, see: *Goodman,* Spam: Technologies and Politics, 2003, available at: http://research.microsoft.com/~joshuago/spamtech.pdf. Regarding user-oriented spam prevention techniques, see: *Rotenberg/Liskow*, ITU WSIS Thematic Meeting On Countering Spam Consumer Perspectives On Spam: Challenges And Challenges, available at: www.itu.int/osg/spu/spam/contributions/Background%20Paper_A%20consumer%20perspective%20on%20spam.pdf.

[1836] Spam Issues in Developing Countries, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1837] See Spam Issues in Developing Countries, page 4, available at: www.oecd.org/dataoecd/5/47/34935342.pdf.

[1838] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 37, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[1839] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 69: "The sending of unsolicited e-mail, for commercial or other purposes, may cause nuisance to its recipient, in particular when such messages are sent in large quantities or with a high frequency ("spamming"). In the opinion of the drafters, such conduct should only be criminalised where the communication is intentionally and seriously hindered. Nevertheless, Parties may have a different approach to hindrance under their law, e.g. by making particular acts of interference administrative offences or otherwise subject to sanction. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered – partially or totally, temporarily or permanently – to reach the threshold of harm that justifies sanction, administrative or criminal, under their law."

[1840] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in Seymour/Goodman, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1841] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1842] The document available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1843] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1844] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1845] Regarding the US legislation on spam, see: *Sorkin*, Spam Legislation in the United States, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Warner*, Spam and Beyond: Freedom, Efficiency, and the Regulation of E-mail Advertising, The John Marshall Journal of Computer & Information Law, Vol. XXII, 2003; *Alongi*, Has the US conned Spam, Arizona Law Review, Vol. 46, 2004, page 263 *et seq.*, available at: www.law.arizona.edu/Journals/ALR/ALR2004/vol462/alongi.pdf; Effectiveness and Enforcement of the CAN-SPAM Act: Report to Congress, 2005, available at: http://www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

[1846] For more details about the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM act 2003), see: www.spamlaws.com/f/pdf/pl108-187.pdf.

[1847] See: *Hamel,* Will the CAN-SPAM Act of 2003 Finally Put a Lid on Unsolicited E-mail?, New Eng. Law Review, 39, 2005, 196 *et seq.* 325, 327 (2001).

[1848] For more details, see: *Bueti,* ITU Survey on Anti-Spam legislation worldwide 2005, available at: www.itu.int/osg/spu/spam/legislation/Background_Paper_ITU_Bueti_Survey.pdf.

[1849] For more information, see: *Wong,* The Future Of Spam Litigation After Omega World Travel v. Mummagraphics, Harvard Journal of Law & Technology, Vol. 20, No. 2, 2007, page 459 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v20/20HarvJLTech459.pdf.

[1850] Websense Security Trends Report 2004, page 11, available at: www.websense.com/securitylabs/resource/WebsenseSecurityLabs20042H_Report.pdf; Information Security – Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3, available at: www.globalsecurity.org/security/library/report/gao/d03837.pdf; *Sieber*, Council of Europe Organised Crime Report 2004, page 143.

[1851] One example of this misuse is the publication of passwords used for access control. Once published, a single password can grant access to restricted information to hundreds of users.

[1852] One example is the 2001 EU Framework Decision combating fraud and counterfeiting of non-cash means of payment.

[1853] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 71: "To combat such dangers more effectively, the criminal law should prohibit specific potentially dangerous acts at the source, preceding the commission of offences under Articles 2 – 5. In this respect the provision builds upon recent developments inside the Council of Europe (European Convention on the legal protection of services based on, or consisting of, conditional access – ETS N° 178) and the European Union (Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access) and relevant provisions in some countries".

[1854] With the definition of "distributing" in the Explanatory Report ('Distribution' refers to the active act of forwarding data to others – Explanatory Report, No. 72), the drafters of the Convention restrict devices to software. Although the Explanatory Report is not definitive in this matter, it is likely that it covers not only software devices, but hardware tools as well.

[1855] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

[1856] See, in this context: *Biancuzzi*, The Law of Full Disclosure, 2008, available at: www.securityfocus.com/print/columnists/466.

[1857] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society:

Article 6 – Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

[1858] See for example one approach in the US legislation:

18 USC. § 1029 (Fraud and related activity in connection with access devices)

(a) Whoever -

(1) knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;

(2) knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;

(3) knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;

(4) knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;

(5) knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of -

(A) offering an access device; or

(B) selling information regarding or an application to obtain an access device;

(7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)

(1) Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

(2) Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both. […]

1859 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

1860 This approach could lead to broad criminalization. Therefore Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

1861 Art. 6, Subparagraph 3 of the Convention on Cybercrime enables states to make a reservation and limit criminalization to the distribution, sale and making available of devices and passwords.

1862 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72.

1863 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 72: "*This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices*".

1864 Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001, on the harmonization of certain aspects of copyright and related rights in the information society.

1865 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 73: The drafters debated at length whether the devices should be restricted to those which are designed exclusively or specifically for committing offences, thereby excluding dual-use devices. This was considered to be too narrow. It could lead to insurmountable difficulties of proof in criminal proceedings, rendering the provision practically inapplicable or only applicable in rare instances. The alternative to include all devices even if they are legally produced and distributed, was also rejected. Only the subjective element of the intent of committing a computer offence would then be decisive for imposing a punishment, an approach which in the area of money counterfeiting also has not been adopted. As a reasonable compromise the Convention restricts its scope to cases where the devices are objectively designed, or adapted, primarily for the purpose of committing an offence. This alone will usually exclude dual-use devices.

1866 Regarding the US approach to address the issue, see for example 18 USC. § 2512 (2):

(2) It shall not be unlawful under this section for –

(a) a provider of wire or electronic communication service or an officer, agent, or employee of, or a person under contract with, such a provider, in the normal course of the business of providing that wire or electronic communication service, or

(b) an officer, agent, or employee of, or a person under contract with, the United States, a State, or a political subdivision thereof, in the normal course of the activities of the United States, a State, or a political subdivision thereof, to send through the mail, send or carry in interstate or foreign commerce, or manufacture, assemble, possess, or sell any electronic, mechanical, or other device knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications.

1867 *Gercke*, Cybercrime Training for Judges, 2009, page 39, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

1868 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76: "Paragraph 2 sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and

network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'."

[1869] See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 731.

[1870] See, for example, the World Information Technology And Services Alliance (WITSA) Statement On The Council Of Europe Draft Convention On Cyber-Crime, 2000, available at: www.witsa.org/papers/COEstmt.pdf; Industry group still concerned about draft Cybercrime Convention, 2000, available at: www.out-law.com/page-1217.

[1871] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[1872] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 76.

[1873] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1874] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 77.

[1875] For more information, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 78.

[1876] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: http://www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[1877] Expert Group's suggestion for an amendment:

Paragraph 3:

A person who possesses more than one item mentioned in subparagraph (i) or (ii), is deemed to possess the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6,7 or 8 unless the contrary is proven.

Official Note: Subsection 3 *is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context*.

[1878] Canada's suggestion for an amendment:

Paragraph 3:

(3) Where a person possesses more than [number to be inserted] item(s) mentioned in subparagraph (i) or (ii), a court may infer that the person possesses the item with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8, unless the person raises a reasonable doubt as to its purpose.

Official Note: Subsection 3 *is an optional provision. For some countries such a presumption may prove very useful while for others, it may not add much value, in the context of this particular offence. Countries need to consider whether the addition would be useful within the particular legal context*.

[1879] The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International

Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1880] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1881] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1882] "Draft thereby makes criminal the knowing and deliberate effort to cause illegal attacks through such distribution, but not discussions of computer vulnerability intended for evaluating." See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1883] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1884] See *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.88.

[1885] See for example: *Austria*, Forgery in Cyberspace: The Spoof could be on you, University of Pittsburgh School of Law, Journal of Technology Law and Policy, Vol. IV, 2004, available at: http://tlp.law.pitt.edu/articles/Vol5-Austria.pdf.

[1886] See for example 18 USC. § 495:

Whoever falsely makes, alters, forges, or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving, or of enabling any other person, either directly or indirectly, to obtain or receive from the United States or any officers or agents thereof, any sum of money; or Whoever utters or publishes as true any such false, forged, altered, or counterfeited writing, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited; or

Whoever transmits to, or presents at any office or officer of the United States, any such writing in support of, or in relation to, any account or claim, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited –

Shall be fined under this title or imprisoned not more than ten years, or both.

Or Sec. 267 German Penal Code:

Section 267 Falsification of Documents

(1) Whoever, for the purpose of deception in legal relations, produces a counterfeit document, falsifies a genuine document or uses a counterfeit or a falsified document, shall be punished with imprisonment for not more than five years or a fine.

(2) An attempt shall be punishable.

(3) In especially serious cases the punishment shall be imprisonment from six months to ten years. An especially serious cases exists, as a rule, if the perpetrator:

1. acts professionally or as a member of a gang which has combined for the continued commission of fraud or falsification of documents;
2. causes an asset loss of great magnitude;
3. substantially endangers the security of legal relations through a large number of counterfeit or falsified documents; or
4. abuses his powers or his position as a public official.

(4) Whoever commits the falsification of documents professionally as a member of a gang which has combined for the continued commission of crimes under Sections 263 to 264 or 267 to 269, shall be punished with imprisonment from one year to ten years, in less serious cases with imprisonment from six months to five years.

[1887] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 82.

[1888] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 81: "The purpose of this article is to create a parallel offence to the forgery of tangible documents. It aims at filling gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Manipulations of such data with evidentiary value may have the same serious consequences as traditional acts of forgery if a third party is thereby misled. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception."

1889 See Art. 1 (b) Convention on Cybercrime.

1890 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

1891 For example, by filling in a form or adding data to an existing document.

1892 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 84.

1893 With regard the definition of "alteration" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1894 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

1895 With regard the definition of "suppression" in Art. 4, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1896 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

1897 With regard the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1898 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 83.

1899 If only part of a document is deleted the act might also be covered by the term "alteration".

1900 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1901 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

1902 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1903 See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 85.

1904 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1905 The Stanford Draft International Convention (CISAC) was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1906 See, for example: *Thorne/Segal*, Identity Theft: The new way to rob a bank, CNN, 22.05.2006, available at: http://edition.cnn.com/2006/US/05/18/identity.theft/; Identity Fraud, NY Times Topics, available at: http://topics.nytimes.com/top/reference/timestopics/subjects/i/identity_fraud/index.html; *Stone*, US Congress looks at identity theft, International Herald Tribune, 22.03.2007, available at: http://www.iht.com/articles/2007/03/21/business/identity.php.

[1907] See, for example, the 2007 Javelin Strategy and Research Identity Fraud Survey; 2006 Better Bureau Identity Fraud Survey; 2006 Federal Trade Commission Consumer Fraud and Identity Theft Complaint Data; 2003 Federal Trade Commission Identity Theft Survey Report.

[1908] See, for example: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf; *Peeters*, Identity Theft Scandal in the US: Opportunity to Improve Data Protection, Multimedia und Recht 2007, page 415; *Givens*, Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions, 2000, available at: www.privacyrights.org/ar/id_theft.htm.

[1909] Regarding the phenomenon of identity theft, see above: § 2.8.3.

[1910] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

[1911] Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cybercrime, COM (2007) 267.

[1912] *Gercke*, Legal Approaches to Criminalize Identity Theft, Commission on Crime Prevention and Criminal Justice, Document No: E/CN.15/2009/CRP.13, page 8 *et seq.*

[1913] *Gercke*, Internet-related Identity Theft, 2007, available at: www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

[1914] This is not the case if the scam is based solely on synthetic data. Regarding the relevance of synthetic data, see: *McFadden*, Synthetic identity theft on the rise, Yahoo Finance, 16.05.2007, available at: http://biz.yahoo.com/brn/070516/21861.html?.v=1=1 ; ID Analytics, http://www.idanalytics.com/assets/pdf/National_Fraud_Ring_Analysis_Overview.pdf.

[1915] The reason for the success is the fact that the provisions focus on the most relevant aspect of phase 1: transfer of the information from the victim to the offender.

[1916] Examples of acts that are not covered include the illegal access to a computer system in order to obtain identity related information.

[1917] One of the most common ways the information obtained is used is fraud. See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3, available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[1918] Furthermore, it is uncertain whether the provisions criminalize possession if the offender does not intend to use the data but to sell them. Prosecution could in this case in general be based on fact that 18 USC. § 1028 not only criminalizes possession with the intent to use it to commit a crime, but also to aid or abet any unlawful activity.

[1919] The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1920] Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

[1921] See also: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006, page 29, available at: www.lex-electronica.org/articles/v11-1/chawki_abdel-wahab.pdf.

[1922] Similar provisions are included in the Commonwealth Model Law and the Stanford Draft International Convention. For more information about the Commonwealth model law, see: Model Law on Computer and Computer Related Crime, LMM(02)17. The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf. For more information about the Stanford Draft International Convention, see: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an

International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1923] See above: § 6.1.1.

[1924] See above: § 6.1.4.

[1925] See above: § 6.1.5.

[1926] *Mitchison/Wilikens/Breitenbach/Urry/Portesi* – Identity Theft – A discussion paper, page 23, available at: www.prime-project.eu/community/furtherreading/studies/IDTheftFIN.pdf.

[1927] See: Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

[1928] See above: § 2.8.1.

[1929] Regarding the criminalization of computer-related fraud in the UK, see: *Walden*, Computer Crimes and Digital Investigations, 2006, Chapter 3.50 *et seq.*

[1930] One example of this is Section 263 of the German Penal Code that requires the falsity of a person (mistake). The provision does not therefore cover the majority of computer-related fraud cases:

Section 263 Fraud

(1) Whoever, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the assets of another, by provoking or affirming a mistake by pretending that false facts exist or by distorting or suppressing true facts, shall be punished with imprisonment for not more than five years or a fine.

[1931] A national approach that is explicitly address computer-related fraud is 18 USC. § 1030:

Sec. 1030. Fraud and related activity in connection with computers

(a) Whoever -

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains -

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

[1932] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

[1933] The drafters highlighted that the four elements have the same meaning as in the previous articles: "To ensure that all possible relevant manipulations are covered, the constituent elements of 'input', 'alteration', 'deletion' or 'suppression' in Article 8(a) are supplemented by the general act of 'interference with the functioning of a computer

program or system' in Article 8(b). The elements of 'input, alteration, deletion or suppression' have the same meaning as in the previous articles." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

1934 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 86.

1935 With regard to the definition of "alteration" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1936 With regard to the definition of "suppression" in Art. 4, see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1937 With regard to the definition of "deletion", see Explanatory Report to the Council of Europe Convention on Cybercrime, No. 61.

1938 As a result, not only data-related offences, but also hardware manipulations, are covered by the provision.

1939 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 87.

1940 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 88.

1941 "The offence has to be committed "intentionally". The general intent element refers to the computer manipulation or interference causing loss of property to another. The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another."

1942 The drafters of the Convention point out that these acts are not meant to be included in the offence established by Article 8 – Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

1943 The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report notes that: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

1944 Explanatory Report to the Council of Europe Convention on Cybercrime, No. 90.

1945 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

1946 The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

1947 Regarding the ongoing transition process, see: OECD Information Technology Outlook 2006, Highlights, page 10, available at: www.oecd.org/dataoecd/27/59/37487604.pdf.

1948 For more information on the effects of digitization on the entertainment industry, see above: § 2.7.1.

[1949] The technology that is used is called digital rights management – DRM. The term digital rights management (DRM) is used to describe several technologies used to enforce pre-defined policies controlling access to software, music, movies or other digital data. One of the key functions is copy protection, which aims to control or restrict the use and access to digital media content on electronic devices with such technologies installed. For further information, see: *Cunard/Hill/Barlas*, Current developments in the field of digital rights management, available at: www.wipo.int/documents/en/meetings/2003/sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View, available at: www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

[1950] Regarding the technical approach to copyright protection, see: *Persson/Nordfelth*, Cryptography and DRM, 2008, available at: www.it.uu.se/edu/course/homepage/security/vt08/drm.pdf.

[1951] For details see above: § 2.7.1.

[1952] Examples are 17 USC. § 506 and 18 USC. § 2319:

Section 506. Criminal offenses

(a) Criminal Infringement. — Any person who infringes a copyright willfully either –

(1) for purposes of commercial advantage or private financial gain, or

(2) by the reproduction or distribution, including by electronic means, during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000, shall be punished as provided under section 2319 of title 18, United States Code. For purposes of this subsection, evidence of reproduction or distribution of a copyrighted work, by itself, shall not be sufficient to establish willful infringement.

[...]

Section 2319. Criminal infringement of a copyright

(a) Whoever violates section 506(a) (relating to criminal offenses) of title 17 shall be punished as provided in subsections (b) and (c) of this section and such penalties shall be in addition to any other provisions of title 17 or any other law.

(b) Any person who commits an offense under section 506(a)(1) of title 17 –

(1) shall be imprisoned not more than 5 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution, including by electronic means, during any 180-day period, of at least 10 copies or phonorecords, of 1 or more copyrighted works, which have a total retail value of more than $2,500;

(2) shall be imprisoned not more than 10 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, in any other case.

(c) Any person who commits an offense under section 506(a)(2) of title 17, United States Code –

(1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;

(2) shall be imprisoned not more than 6 years, or fined in the amount set forth in this title, or both, if the offense is a second or subsequent offense under paragraph (1); and

(3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.

(d)(1) During preparation of the presentence report pursuant to Rule 32(c) of the Federal Rules of Criminal Procedure, victims of the offense shall be permitted to submit, and the probation officer shall receive, a victim impact statement that identifies the victim of the offense and the extent and scope of the injury and loss suffered by the victim, including the estimated economic impact of the offense on that victim.

(2) Persons permitted to submit victim impact statements shall include –

(A) producers and sellers of legitimate works affected by conduct involved in the offense;

(B) holders of intellectual property rights in such works; and

(C) the legal representatives of such producers, sellers, and holders.

(e) As used in this section –

(1) the terms "phonorecord" and "copies" have, respectively, the meanings set forth in section 101 (relating to definitions) of title 17; and

(2) the terms "reproduction" and "distribution" refer to the exclusive rights of a copyright owner under clauses (1) and (3) respectively of section 106 (relating to exclusive rights in copyrighted works), as limited by sections 107 through 122, of title 17.

Regarding the development of legislation in the United States, see: *Rayburn*, After Napster, Virginia Journal of Law and Technology, Vol. 6, 2001, available at: www.vjolt.net/vol6/issue3/v6i3-a16-Rayburn.html.

[1953] Regarding the international instruments, see: *Sonoda*, Historical Overview of Formation of International Copyright Agreements in the Process of Development of International Copyright Law from the 1830s to 1960s, 2006, available at: www.iip.or.jp/e/summary/pdf/detail2006/e18_22.pdf; *Okediji*, The International Copyright System: Limitations, Exceptions and Public Interest Considerations for Developing Countries, 2006, available at: www.unctad.org/en/docs/iteipc200610_en.pdf. Regarding international approaches to anti-circumvention laws, see: *Brown*, The evolution of anti-circumvention law, International Review of Law, Computer and Technology, 2006, available at: www.cs.ucl.ac.uk/staff/I.Brown/anti-circ.pdf.

[1954] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 109.

[1955] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 110: "With regard to paragraph 1, the agreements referred to are the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the World Intellectual Property Organisation (WIPO) Copyright Treaty. With regard to paragraph 2, the international instruments cited are the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) and the World Intellectual Property Organisation (WIPO) Performances and Phonograms Treaty. The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

[1956] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 111: "The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the current Convention is not bound to apply agreements cited to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention."

[1957] Explanatory Report to the Council of Europe Convention on Cybercrime, Nos. 16 and 108.

[1958] *Article 61:*

Members shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale. Remedies available shall include imprisonment and/or monetary fines sufficient to provide a deterrent, consistently with the level of penalties applied for crimes of a corresponding gravity. In appropriate cases, remedies available shall also include the seizure, forfeiture and destruction of the infringing goods and of any materials and implements the predominant use of which has been in the commission of the offence. Members may provide for criminal procedures and penalties to be applied in other cases of infringement of intellectual property rights, in particular where they are committed wilfully and on a commercial scale.

[1959] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 113.

[1960] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 114.

[1961] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime. The Explanatory Report points out: "*A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability. The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. The Convention, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences). Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised*". See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 38.

[1962] See Explanatory Report to the Council of Europe Convention on Cybercrime, No. 115. In addition, the drafters pointed out: The absence of the term "without right" does not *a contrario* exclude application of criminal law defences, justifications and principles governing the exclusion of criminal liability associated with the term "without right" elsewhere in the Convention.

[1963] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[1964] See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1965] See: *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[1966] See, for example, Art. 5 of the Convention on Cybercrime.

[1967] Convention on Cybercrime, ETS 185.

[1968] Council of Europe Convention on the Prevention of Terrorism, ETS 196.

[1969] Council of Europe Convention on the Prevention of Terrorism, ETS 196.

[1970] EU Framework Decision on Combating Terrorism, COM (2007) 650.

[1971] EU Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism.

[1972] EU Framework Decision 2008/919/JHA of 28 November 2008, No. 4.

[1973] The intention of the drafters to cover online and offline activities was highlighted several times. See, for example: EU Framework Decision 2008/919/JHA of 28 November 2008, No. 11. "These forms of behavior should be equally punishable in all Member States irrespective of whether they are committed through the Internet or not."

[1974] Regarding the motivation, see: *Russell*, A History of the United Nations Charter, 1958.

[1975] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

[1976] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 59.

[1977] *Mani*, Basic Principles of Modern International Law: A Study of the United Nations Debates on the Principles of International Law Concerning Friendly Relations and Co-operation among States, 1993, page 263 *et seq.*

[1978] *Bond*, Peacetime foreign Data Manipulations as one Aspect of Offensive Information Warfare, 1996.

[1979] *Brownlie*, International Law and the Use of Force, 1993, page 362.

[1980] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 80.

[1981] *Solce*, The Battlefield of Cyberspace: The inevitable new military branch – the cyber force, Alb. Law Journal of Science and Technology, Vol. 18, page 304.

[1982] *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 57.

[1983] *Albright/Brannan/Waldrond*, Did Stuxnet Take out 1 000 Centrifuges at the Nataz Enrichment Plant?, Preliminary Assessment, Institute for Science and International Security, 2010.

[1984] Regarding proliferation concerns, see: *Barkham*, Information Warfare and international Law on the use of Force, International Law and Politics, Vol. 34, page 58.

[1985] With regard to the development, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[1986] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No.5.

[1987] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 6.

[1988] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[1989] Regarding the admissibility and reliability of digital images, see: *Witkowski*, Can Juries Really Believe What They See? New Foundational Requirements for the Authentication of Digital Images, Journal of Law & Policy, page 267 *et seq.*

[1990] *Harrington*, A Methodology for Digital Forensics, T.M. Cooley J. Prac. & Clinical L., 2004, Vol. 7, page 71 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 14. Regarding the legal frameworks in different countries, see: *Rohrmann/Neto*, Digital Evidence in Brazil, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Wang*, Electronic Evidence in China, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Bazin*, Outline of the French Law on Digital Evidence, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Makulilo*, Admissibility of Computer Evidence in Tanzania, Digital Evidence and Electronic Signature Law Review, 2008, No. 5; *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 76; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213.

[1991] See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

[1992] For a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

[1993] The Council of Europe Convention on Cybercrime therefore contains a provision that clarifies that the procedural instruments in the Convention shall not only be applicable with regard to cybercrime-related offences, but also to "other criminal offences committed by means of a computer system" and "the collection of evidence in electronic form of a criminal offence" (Art. 14).

[1994] *Casey*, Digital Evidence and Computer Crime, 2004, page 9.

[1995] Regarding the need for formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

[1996] Regarding the difficulties of dealing with digital evidence on the basis of traditional procedures and doctrines, see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 *et seq.*

[1997] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 3. Regarding the early discussion about the use of printouts, see: *Robinson*, The Admissibility of Computer Printouts under the Business Records Exception in Texas, South Texas Law Journal, Vol. 12, 1970, page 291 *et seq.*

[1998] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, page 1.

[1999] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1. Regarding the historical development of computer forensics and digital evidence, see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[2000] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286. With more reference to national law: *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 213; *Vaciago*, Digital Evidence, 2012, Chapter I.1 (with an overview about the discussion about digital evidence in different jurisdictions).

[2001] Police and Criminal Evidence Code (PACE).

[2002] *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm.

[2003] Regarding the different models of cybercrime investigation, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

[2004] This includes the development of investigation strategies.

[2005] The second phase covers, in particular, the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2006] See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

[2007] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 532.

[2008] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[2009] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[2010] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2011] This includes, for example, the reconstruction of operating processes. See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

[2012] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2013] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process within forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

[2014] Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

[2015] *Vaciago*, Digital Evidence, 2012, Chapter II.

[2016] *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

[2017] Regarding geo-recognition, see: *Friedland/Sommer*; Cybercasing the Joint: On the Privacy Implications of Geo-Tagging, available at: www.icsi.berkeley.edu/pubs/networking/cybercasinghotsec10.pdf; *Strawn*, Expanding the Potential for GPS Evidence Acquisition, Small Scale Digital Device Forensics Journal, 2009, Vol. 3, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V3_1_Strawn.pdf; *Zdziarski*, iPhone Forensics, 2008, available at: www.esearchbook.com/files/4/eSearchBook.1224255173.iPhone%20Forensics.pdf.

[2018] See *Liberatore/Erdely/Kerle/Levine/Shields*, Forensic investigation of peer-to-peer file sharing networks, Digital Investigations, 2010, page 95 *et seq.*, available at: www.dfrws.org/2010/proceedings/2010-311.pdf.

[2019] Regarding the use of metadata for investigations, see: *Luque*, Logical Level Analysis of Unix Systems in: Handbook of Computer Crime Investigations: Forensic Tools and Technology, 2001; *Cohen*, Digital Still Camera Forensics, Small Scale Digital Device Forensics Journal, 2007, Vol. 1, No. 1, available at: www.ssddfj.org/papers/SSDDFJ_V1_1_Cohen.pdf.

[2020] *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

[2021] *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217. Regarding the challenges of witnesses as a source of evidence, see: *Walton*, Witness Testimony Evidence: Argumentation and the Law, 2007; *Heaton-Armstrong/Shepherd/Wolchover*, Analysing Witness Testimony: Psychological, Investigative and Evidential Perspective, 2002.

[2022] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2023] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 19.

[2024] Regarding the liability of digital investigations, see: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

[2025] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161.

[2026] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2027] *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2028] Daubert v. Merrell Dow Pharmaceutical, Inc. (1993) 113 S. Ct. 2786, available at: http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=509&invol=579.

[2029] *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No. 3, page 1.

[2030] The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

[2031] Regarding the status of national legislation, see for example: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[2032] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[2033] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[2034] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

[2035] *Casey*, Digital Evidence and Computer Crime, 2004, page 15.

[2036] *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2Dpage 38F31AF079F9.pdf; With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2037 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf. Criteria for Admissibility of Expert Opinion, Utah Law Review, 1978, page 546 *et seq.*

2038 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

2039 See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.

2040 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 217.

2041 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2042 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

2043 See Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten, Lest We Remember: Colt Boot Attacks on Encryption Keys.

2044 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 92.

2045 *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

2046 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2047 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2048 *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

2049 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2050 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2051 For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

2052 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2053 *Castelluccia/Cristofaro/Perito*, Private Information Disclosure from Web Searches, The Case of Google Web History, 2010, available at: http://planete.inrialpes.fr/~ccastel/PAPERS/historio.pdf; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/EFE47BD9-A897-6585-5EAB032ADF89EDCF.pdf.

2054 *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

2055 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2056 *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

2057 Regarding the design of courtrooms, see: *Youngblood*, Courtroom Design, 1976; *Smith/Larson*, Courtroom design, 1976.

2058 Scientific Evidence Review: Admissibility of Expert Evidence, ABA, 2003, page 159 *et seq.*; *Casey*, Digital Evidence and Computer Crime, 2004, page 169; *Nilsson*, Digital Evidence in the Courtroom, 2010; *Rabinovich-Einy*, Beyond Efficiency: The Transformation of Courts Through Technology, UCLA Journal of Law & Technology, 2008, Vol. 12, Issue 1.

2059 *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

2060 See *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol. 119, page 538.

2061 Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

2062 *Casey*, Digital Evidence and Computer Crime, 2004, page 20.

2063 *Gercke*, Impact of Cloud Computing on the work of law-enforcement agencies, published in Taeger/Wiebe, Inside the Cloud, 2009, page 499 *et seq.*

2064 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 218.

2065 *Insa*, The Admissibility of Electronic Evidence in Court: Fighting against High-Tech Crime – Results of a European Study, Journal of Digital Forensic Practice, 2006, page 286.

2066 See in this context: *Nikali*, The Substitution of Letter Mail in Targeted Communication, 2007, available at: http://hsepubl.lib.hse.fi/pdf/diss/a136.pdf.

2067 See in this context *Morris*, Forensic Handwriting Identification: Fundamental Concepts and Principles, 2000; *Ellen*, Scientific Examination of Documents: Methods and Techniques, 2005; *Hayes*, Forensic Handwriting Examination, 2006.

2068 *Houck/Siegel*, Fundamentals of Forensic Science, 2010, page 512 *et seq.*; FBI Handbook of Crime Scene Forensics, 2008, page 111 *et seq.*; *Hilton*, Identification of the Work from an IBM Selectric Typewriter, Journal of Forensic Sciences, 1962, Vol. 7, Issue 3, page 286 *et seq.*; *Miller*, An Analysis of the Identification Value of Defects in IBM Selectric Typewriters, American Academy of Forensic Science annual meeting, presented paper, Ohio, 1983; *Koppenhaver*, Forensic Document Examination: Principles and Practice, 2007, page 207 *et seq.*

2069 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

2070 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mail: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, Issue 4, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B4342D-E76E-F8F2-AC926AB64EC719B8.pdf.

2071 *Meghanathan/Allam/Moore*, Tools and Techniques for Network Forensics, International Journal of Network Security and its Applications, 2009, Vol. 1, No. 1, page 16 *et seq.*, available at: http://airccse.org/journal/nsa/0409s2.pdf.

2072 *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

2073 Regarding approaches to link a suspect to stored computer records, see for example: *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 165.

2074 Regarding the obligation to register prior to the use of public Internet terminals in Italy, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, CRi 2006, page 94.

2075 See: *Richtel*, Live Tracking of Mobile Phones Prompts Court Fight on Privacy, The New York Times, 10.12.2005, available at: www.nytimes.com/2005/12/10/technology/10phone.html?pagewanted=print10dec2005. Regarding the legal implications, see: *Samuel*, Warrantless Location Tracking, New York University Law Review, 2008, Vol. 38, page 1324 *et seq.*, available at www.law.nyu.edu/ecm_dlv4/groups/public/@nyu_law_website__journals__law_review/documents/web_copytext/ecm_pro_059784.pdf.

2076 Regarding a case where search-engine requests were used as evidence in a murder case, see: *Jones*, Murder Suspect's Google Search Spotlighted in Trial, Informationweek.com, 11.11.2005, available at: www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=173602206.

2077 Regarding the extent of commercial child pornography, see: IWF 2007 Annual and Charity Report, page 7.

2078 See *Schnabel,* The Mikado Principle, Datenschutz und Datensicherheit, 2006, page 426 *et seq.*

2079 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 206.

2080 Regarding the legitimacy principle, see: *Grans/Palmer*, Australian Principles of Evidence, 2005, page 10.

2081 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 219.

2082 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 207.

2083 *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

2084 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

2085 Regarding necessary procedures, see: *Chawki*, The Digital Evidence in the Information Era, available at: www.droit-tic.com/pdf/digital_evid.pdf; *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

2086 *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

2087 *Menezes*, Handbook of Applied Cryptography, 1996, page 361.

2088 *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2089 See in this context also: *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208.

2090 Regarding the consequences of the fruit of the poisonous tree doctrine for computer-crime investigations, see: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 563.

2091 *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

2092 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332 and *Omychund v Barker* (1744) 1 Atk 21 at 49; *Robinson Bros (Brewers) Ltd v. Houghton and Chester-le-Street Assessment Committee* [1937] 2 KB 445 at 468, [1937] 2 All ER 298 at 307, CA, per Scott LJ.

2093 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006, pages 331-332.

2094 *Springsteen v Masquerade Music Ltd* [2001] EWCA Civ 563, [2001] EMLR 654. The primary evidence rule was in any event inapplicable to recordings on film or tape, which may be proven by copies under common law (*Kajala v Noble* (1982) 75 Cr App Rep 149, DC; R v. Wayte (1982) 76 Cr App Rep 110, CA) and if lost or destroyed their contents may be proven by oral evidence from persons who have previously viewed or heard them (*Taylor v Chief Constable of Cheshire* [1987] 1 All ER 225, 84 Cr App Rep 191, DC). Also, see now the Criminal Justice Act 2003 s 133; and para 1464 post.

2095 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; *Permanent Trustee Co of New South Wales v Fels* [1918] AC 879, PC.

2096 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, pages 565-566; The admission of documentary copies is subject to the Civil Evidence Act 1995: see PARA 808 *et seq.*

2097 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

2098 *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

2099 With regard to different exemptions, see: *Nemeth*, Law of Evidence: A Primer for Criminal Justice, 2007, page 144 *et seq.*; Best Evidence Rule, California Law Review Commission, 1996, available at: www.clrc.ca.gov/pub/Printed-Reports/REC-BestEvidenceRule.pdf; *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

2100 For further reference, see: *Eltgroth*, Best Evidence and the Wayback Machine, Fordham Law Review, 2009, 193, available at: http://law.fordham.edu/assets/LawReview/Eltgroth_October_2009.pdf.

2101 With regard to European common law countries (UK, Ireland), this development was especially supported by EU Directive 1999/93/EC. See also Sec. 4 and 6 of the Commonwealth model law on electronic evidence.

2102 *Munday*, Evidence, 2007, page 380; *Allen*, Practical Guide to Evidence, 2008, page 189.

2103 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567.

2104 Halsbury's Laws of England, Vol. 11: Civil Procedure, 2009, page 567 and *R v Sharp* [1988] 1WLR 7, HL; *R v Kearley* [1992] 2 AC 228, [1992] 2 All ER 345. HL. See also Civil Evidence Act 1995 ss1-7.

2105 Per Lord Havers in *R v Sharp* [1988] 1 WLR 7 and per Lords Ackner and Oliver in R v Kearley [1992] 2 All ER 345 at 363 and 366 respectively. The rule also extends to out-of-court statements of otherwise admissible opinion.

2106 *Keane*, Modern Law of Evidence, 2005, pages 246-266.

2107 *Dennis*, The Law of Evidence, 2002, Chapters 16-17.16-17.

2108 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

2109 Halsbury's Laws of England, Vol. 11(3): Criminal Law, Evidence and Procedure, 2006.

2110 See in this context, for example, Part II of the Irish Criminal Evidence Act 1992.

2111 R v Dodson [1984] 1 WLR 971, 79 CrApp Rep 220, CA (photographic evidence); R v Maqsud Ali [1966] 1 QB 688, 49 Cr App Rep 230, CCA (tape recorded conversation); R v Wood (1982) 76 Cr App Rep 23, CA; Castle v Cross [1984] 1 WLR 1372, DPP v McKeown [1997] 1 All ER 737, 2 Cr App Rep 155, HL (computer evidence).

2112 A "statement" is now defined as any representation of fact or opinion made by a person by whatever means; and it includes a representation made in a sketch, photo or other pictorial form: Criminal Justice Act 2003 ss 115(2), 134 (2).

2113 See in this context, for example, the Statue of Liberty case, [1968] 1 W.L.R. 739.

2114 *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 246.

2115 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

2116 *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

2117 *Insa/Lazaro*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 214; *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 205.

2118 Model Law on Electronic Evidence (LMM(02)12.

2119 Singapore Evidence Act, Section 35.

2120 Canada Uniform Electronic Evidence Act.

2121 See above.

2122 Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures. For more information, see: *Dumortier*, The European Directive 1999/93/EC on a Community Framework for Electronic Signatures, in Lodder/Kaspersen, eDirectives, 2000, page 33 *et seq.*, available at: www.law.kuleuven.be/icri/publications/58The%20European%20Directive%201999.pdf.

[2123] *Kenneally*, UCLA Journal of Law and Technology, 2005, Vol. 9, Issue 2; *Keane*, Modern Law of Evidence, 2005, page 27.

[2124] *Galves*, Where the not-so-wild things are: Computers in the Courtroom, the Federal Rules of Evidence, and the Need for Institutional Reform and More Judicial Acceptance, Harvard Journal of Law & Technology, 2000, Vol. 13, No. 2, page 238.

[2125] *Clough*, The Admissibility of Digital Evidence, 2002, available at: www.law.monash.edu.au/units/law7281/module5/digital_evidence.pdf.

[2126] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: Savona, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, § 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2127] United Nations Report oft he International Law Commission, Fifty-eigth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm

[2128] *Valesco*, Jurisdictional Aspects of Cloud Computing, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20cristos%20cloud.pdf

[2129] For a general overview see: *Kohl*, Jurisdiction and the Internet: Regulatory Competence over Online Activity, 2007; *Zittrain*, Jurisdiction, Internet Law Series, 2005;

[2130] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2131] National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2132] *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 5, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

[2133] *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 6; *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

[2134] *Van Dervort*, International Law and Organizations: An Introduction, 1998, page 254.

[2135] International Court of Justice, Case of S.S."Lotus", Series A – No. 10, 1927, available at: www.icj-cij.org/pcij/serie_A/A_10/30_Lotus_Arret.pdf.

[2136] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.html; Dunn/Krishna-Hensel/Mauer (eds), The Resurgence of the State, Trends and Progress in Cyberspace Governance, 2007, page 69.

[2137] *Kaspersen*, Cybercrime and internet jurisdiction, Council of Europe, 2009, page 8, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf.

[2138] For an overview about relevant case examples for conflicts see: *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 10 et seq.

[2139] *Brenner/Koops*, Approaches to Cybercrime Jurisdiction, Journal of High Technology Law, Vol. 4, No. 1, 2004, page 21.

[2140] See in this regard for example: *Ali/Ragothaman/Bhagavathula/Pendse*, Security Issues in Airplane Data Networks, available at: http://soar.wichita.edu/dspace/bitstream/handle/10057/398/GRASP-4.pdf?sequence=1; The Developments in Satellite Hardware, Satellite Executive Briefing, Vol. 3, No. 12, 2010, available at: www.satellitemarkets.com/pdf/aug10.pdf.

[2141] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2142] See *Krizek*, Protective Principle of Extraterritorial Jurisdiction: A Brief History and an Application of the Principle to Espionage as an Illustration of Current United States Practice, Boston University International Law Journal, 1988, page 337 et seq; *Cameron*, Protective Principle of International Criminal Jurisdiction, 1994.

[2143] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2144] *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72. Regarding the use of the principle within the US see for example United States v. Gallaxy Sports.

[2145] See in this regard below: § 6.2.8.

[2146] *Menthe*, Jurisdiction in Cyberspace: A Theory of International Spaces, Michigan Telecommunications and Technology Law Review, Vol. 4, 1998, page 72.

[2147] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2148] United Nations Report of the International Law Commission, Fifty-eighth session, General Assembly Official Records, Supplement No. 10 (A/61/10), Annex E, available at: http://untreaty.un.org/ilc/reports/2006/2006report.htm.

[2149] See: *Kobrick*, The Ex Post Facto Prohibition and the Exercise of Universal Jurisdiction over International Crimes, Columbia Law Review, Vol 87, 1987, page 1523 et seq; Regarding the discussion about scope and application of the principle of universal jurisdiction within the UN see the information provided by the Sixth Committee, available at: www.un.org/en/ga/sixth/64/UnivJur.shtml.

[2150] For an overview about the implementation of the principle in European countries see: Universal Jurisdiction in Europe – The State of the Art, Human Rights Watch, 2006, available at: www.hrw.org/sites/default/files/reports/ij0606web.pdf.

[2151] See above: §§ 4.5.4 and 6.1.

[2152] This was also highlighted by the drafters of the Council of Europe Convention on Cybercrime, which contains a set of essential investigation instruments. The drafters of the report point out: “Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques”, see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 132. Regarding the substantive criminal law provisions related to cybercrime, see above: § 6.1.

[2153] Regarding the elements of an anti-cybercrime strategy, see above: § 4. Regarding user-based approaches in the fight against cybercrime, see: *Görling*, The Myth Of User Education, 2006, at www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See also the comment made by *Jean-Pierre Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: “More broadly, we have to educate users. They must all understand what they can and can’t do on the Internet and be warned of the potential dangers. As use of the Internet grows, we’ll naturally have to step up our efforts in this respect.”

[2154] Due to the protocols used in Internet communication and worldwide accessibility, there is very little need for a physical presence at the place where a service is physically offered. Due to this independence of place of action and the crime site, many criminal offences related to the Internet are transnational crimes. Regarding the independence of place of action and the result of the offence, see above: § 3.2.7.

[2155] Regarding the challenges of fighting cybercrime, see above: § 3.2.

[2156] The pure fact that the offender is acting from a different country can result in additional challenges for law-enforcement agencies’ investigations even if similar substantive criminal law provisions and procedural law instruments are in place in both countries. In these cases, the investigation nevertheless requires international cooperation between the authorities in both countries, which in general is more time consuming compared to investigations concentrating on a single country.

[2157] See in this context also: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 134.

[2158] For an overview of the current status of the implementation of the Convention on Cybercrime and its procedural law provisions in selected countries, see the country profiles made available on the Council of Europe website: www.coe.int/cybercrime/.

[2159] See Articles 15-21 of the Council of Europe Convention on Cybercrime.

[2160] See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol. 1, No. 2, page 3.

[2161] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21.

[2162] *Hannan,* To Revisit: What is Forensic Computing, 2004, available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4, available at: www.acpr.gov.au/pdf/ACPR_CC3.pdf. Regarding the need for standardization, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, International Journal of Digital Evidence, Vol. 3, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf; *Morgan*, An Historic Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, Vol. 1, Issue 1; *Hall/Davis*, Towards Defining the Intersection of Forensic and Information Technology, International Journal of Digital Evidence, Vol. 4, Issue 1; *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Forensics, International Journal of Digital Evidence, Vol. 3, Issue 2.

[2163] *Patel/Ciarduain*, The impact of forensic computing on telecommunication, IEEE Communications Magazine, Vol. 38, No. 11, 2000, page 64.

[2164] For an overview of different kinds of evidence that can be collected by computer forensic experts, see: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

[2165] *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 538.

[2166] For an overview of different forensic investigation techniques related to the most common technologies, see: *Carney/Rogers*, The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction, International Journal of Digital Evidence, Vol. 2, Issue 4; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf; *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Urnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, Vol. 5, Issue 1; *Marsico/Rogers*, iPod Forensics, International Journal of Digital Evidence, Vol. 4, Issue 2; *Gupta/Mazumdar*; Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, Vol. 2, Issue 4; Hidden Disk Areas: HPA and DCO, International Journal of Digital Evidence, Vol. 5, Issue 1; *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, Vol. 4, Issue 1; *Howard*, Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files, Berkeley Technology Law Journal, Vol. 19, page 1233; *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

[2167] *Harrison/Heuston/Morrissey/Aucsmith/Mocas/Russelle*, A Lesson Learned Repository for Computer Forensics, International Journal of Digital Evidence, Vol. 1, Issue 3.

[2168] Regarding the different models of Cybercrime investigations, see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol. 3, No. 1. See also *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1, who differentiate between six different phases.

[2169] This includes the development of investigation strategies.

[2170] The second phase covers especially the work of the so-called "first responder" and includes the entire process of collecting digital evidence. See: *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2171] With regard to developments, see: *Abramovitch*, A brief history of hard drive control, Control Systems Magazine, EEE, 2002, Vol. 22, Issue 3, page 28 *et seq.*; *Coughlin/Waid/Porter*, The Disk Drive, 50 Years of Progress and Technology Innovation, 2005, available at: www.tomcoughlin.com/Techpapers/DISK%20DRIVE%20HISTORY,%20TC%20Edits,%20050504.pdf.

[2172] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No. 2, 2006, page 161; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol. X, No. 5.

[2173] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[2174] *Vaciago*, Digital Evidence, 2012, Chapter II.1; *Insa*, Situation Report on the Admissibility of Electronic Evidence in Europe, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 220.

[2175] For guidelines on how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[2176] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.

[2177] Regarding investigation techniques, see: *Casey*, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 204, page 283 *et seq.*

[2178] *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, No. 1.

[2179] *Howard*, Don't Cache out your Case: Prosecuting Child Pornography Possession Laws Based on Images located in Temporary Internet Files, Berkeley Technology Law Journal, 2004, Vol. 19, page 1227 *et seq.*; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 54.

[2180] See below: § 6.3.8.

[2181] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 171.

[2182] Regarding the challenges of encryption, see § 3.2.14 as well as *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, Issue 3.

[2183] Regarding possible counter strategies for law enforcement, see: *Haldeman/Schoen/Heninger* and other, Lest we Remember: Cold Boot Attacks on Encryption keys, 2008, available at: http://citp.princeton.edu/memory.

[2184] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[2185] *Vaciago*, Digital Evidence, 2012, Chapter II.1.

[2186] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 43; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 59.

[2187] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2188] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2189] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.

[2190] *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

[2191] *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 473; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38; *Gercke*, Challenges related to the Fight against Cybercrime, Multimedia und Recht, 2008, page 297.

[2192] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the decryption process in forensic investigations, see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.

[2193] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, 2004, Vol. 2, No. 3. Regarding the forensic software magic lantern, developed as a keylogger used by law enforcement in the US, see: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.2001, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

[2194] Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security – available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

[2195] *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, Vol. 9, No. 2.

[2196] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 52.

[2197] For an overview of the debate, see: *Gercke*, The Role of Internet Service Providers in the Fight Against Child Pornography Computer Law Review International, 2009, page 65 *et seq.*

[2198] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 15.

[2199] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 24.

[2200] See *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime – Toward common best-of-breed guidelines?, 2008, available at: www.coe.int/cybercrime/.

[2201] For more information about the Guidelines, see: *Gercke,* The Council of Europe Guidelines for the Cooperation between LEAs and ISPs against Cybercrime, Computer Law Review International, 2008, page 97 *et seq.*

[2202] See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 29.

[2203] See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No. 30.

[2204] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[2205] Regarding the different sources that can be used to extract traffic data, see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 *et seq.*

[2206] Regarding the impact on tracing offenders, see: *Nicoll*, Concealing and Revealing Identity on the Internet in *Nicoll/Prins/Dellen*, Digital Anonymity and the Law, Tensions and Dimensions, 2003, page 99 *et seq.*

[2207] *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, 2002, Vol. 1, No. 3.

[2208] For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses,

19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

2209 *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, No. 4.

2210 For more information, see: *Crumbley/Heitger/Smith*, Forensic and Investigative Accounting, 2005, § 14.12; *Caloyannides*, Privacy Protection and Computer Forensics, 2004, page 149.

2211 The term "phishing" describes an act that is carried out to make targets disclose personal/secret information. It originally described the use of e-mails to "phish" for passwords and financial data from a sea of Internet users. The use of "ph" is linked to popular hacker naming conventions. See *Gercke*, The criminalization of Phishing and Identity Theft, Computer und Recht, 2005, page 606; *Ollmann*, The Phishing Guide: Understanding & Preventing Phishing Attacks, available at: www.nextgenss.com/papers/NISR-WP-Phishing.pdf.

2212 *Casey*, Digital Evidence and Computer Crime, 2004, page 19.

2213 For more information, see: Spiegel Online, Fahnder ueberpruefen erstmals alle deutschen Kreditkarten, 08.01.2007, available at: www.spiegel.de/panorama/justiz/0,1518,457844,00.html.

2214 *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol. 10, No. 3, page 472.

2215 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2216 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 90, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2217 Regarding the need for a formalization of computer forensics, see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol. 3, No. 2, page 2.

2218 *Malaga*, Requirements for the Admissibility in Court of Digital Evidence, in: Syllabus to the European Certificate on Cybercrime and E-Evidence, 2008, page 208 *et seq.*

2219 *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

2220 A denial-of-service (DoS) attacks aims to make a computer system unavailable by saturating it with external communication requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, Understanding Denial-of-Service Attacks, available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks, available at: www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, Analysis of a Denial of Service Attack on TCP; *Houle/Weaver*, Trends in Denial of Service Attack Technology, 2001, available at: www.cert.org/archive/pdf/DoS_trends.pdf.

2221 *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 64, available at: www.cert.org/archive/pdf/FRGCF_v1.3.pdf.

2222 For further information, see: *Provos/Honeyman*, Hide and Seek: An Introduction to Steganography, available at: http://niels.xtdnet.nl/papers/practical.pdf; *Kharrazi/Sencar/Memon*, Image Steganography: Concepts and Practice, available at: http://isis.poly.edu/~steganography/pubs/ims04.pdf; Labs, Developments in Steganography, available at: http://web.media.mit.edu/~jrs/jrs_hiding99.pdf; *Anderson/Petitcolas*, On The Limits of Steganography, available at: www.cl.cam.ac.uk/~rja14/Papers/jsac98-limsteg.pdf; *Curran/Bailey*, An Evaluation of Image Based Steganography Methods, International Journal of Digital Evidence, Vol. 2, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0AD276C-EACF-6F38-E32EFA1ADF1E36CC.pdf.

2223 *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9.

2224 See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.

2225 Botnets is a short term for a group of compromised computers running programs that are under external control. For more details, see *Wilson*, Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress, 2007, page 4, available at: www.fas.org/sgp/crs/terror/RL32114.pdf. See also collected resources and links in the ITU Botnet Mitigation Toolkit, 2008, available at: www.itu.int/ITU-D/cyb/cybersecurity/projects/botnet.html.

2226 With regard to the criminalization of illegal devices, see below: § 6.1.15.

[2227] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.

[2228] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.

[2229] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 29.

[2230] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.

[2231] Regarding the ability to manipulate the time information and the response in forensic investigations, see: *Gladyshev/Patel*, Formalizing Event Time Bounding in Digital Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1. Regarding dynamic time analysis, see: *Weil*, Dynamic Time & Date Stamp Analysis, International Journal of Digital Evidence, 2002, Vol. 1, No. 2.

[2232] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.

[2233] *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2234] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

[2235] See *Casey*, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.

[2236] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf.

[2237] *Whitcomb*, An Historical Perspective of Digital Evidence – A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E695B-0B78-1059-3432402909E27BB4.pdf.

[2238] For an overview of the different techniques, see: *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol. 1, No. 1, page 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Cristopher*, Computer Evidence: Collection and Preservation, 2006.

[2239] Regarding the related procedural instrument, see: Art. 19, paragraph 3 Convention on Cybercrime.

[2240] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 12.

[2241] *Talleur*, Digital Evidence: The Moral Challenge, International Journal of Digital Evidence, 2002, Vol. 1, Issue 1, page 1 *et seq.*, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4E398D-0CAD-4E8D-CD2D38F31AF079F9.pdf. With a strong call for courts looking at experts in forensic investigations: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

[2242] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.

[2243] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 62.

[2244] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 *et seq.*; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 *et seq.*

[2245] See *Gercke*, Convention on Cybercrime, Multimedia und Recht. 2004, page 801, for further reference

[2246] Taylor, The Council of Europe Cybercrime Convention – A civil liberties perspective, available at http://crime-research.org/library/CoE_Cybercrime.html; Cybercrime: Lizenz zum Schnueffeln Financial Times Germany, 31.8.2001; Statement of the Chaos Computer Club, available at www.ccc.de.

[2247] See *Breyer,* Council of Europe Convention on Cybercrime, DUD, 2001, 595 *et seq.*

[2248] Regarding the possibilities of making reservations, see Article 42 of the Convention on Cybercrime:

Article 42

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

2249 See above: § 5.2.1.

2250 "Although Parties are obligated to introduce certain procedural law provisions into their domestic law, the modalities of establishing and implementing these powers and procedures into their legal system, and the application of the powers and procedures in specific cases, are left to the domestic law and procedures of each Party. These domestic laws and procedures, as more specifically described below, shall include conditions or safeguards, which may be provided constitutionally, legislatively, judicially or otherwise. The modalities should include the addition of certain elements as conditions or safeguards that balance the requirements of law enforcement with the protection of human rights and liberties. As the Convention applies to Parties of many different legal systems and cultures, it is not possible to specify in detail the applicable conditions and safeguards for each power or procedure." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

2251 "There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 145.

2252 For the transformation of safeguards for Internet-related investigation techniques, see: *Taylor*, The Scope of Government Access to Copies of Electronic Communication Stored with Internet Service Providers: A Review of Legal Standards, Journal of Technology Law and Policy, Vol. 6, Issue 2, available at: http://grove.ufl.edu/~techlaw/vol6/issue2/taylor.pdf.

2253 This is especially relevant with regard to the protection of the suspect of an investigation.

2254 See: Article 37 – Accession to the Convention.

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2255 ABA International Guide to Combating Cybercrime, page 139.

2256 "Interception of telephone conversations represent[s] a serious interference with private life and correspondence and must accordingly be based upon a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated" – Case of Kruslin v. France, Application No. 11801/85.

2257 "The requirements of the Convention, notably in regard to foreseeability, cannot be exactly the same in the special context of interception of communications for the purposes of police investigations as they are where the object of the relevant law is to place restrictions on the conduct of individuals. In particular, the requirement of foreseeability cannot mean that an individual should be enabled to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly", Case of Malone v. United Kingdom, Application No. 8691/79.

2258 "Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only insofar as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

2259 "The expression "in accordance with the law", within the meaning of Article 8 § 2 (Art. 8-2), requires firstly that the impugned measure should have some basis in domestic law", Case of Kruslin v. France, Application No. 11801/85.

2260 "Furthermore, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject", Case of Doerga v. The Netherlands, Application No. 50210/99.

2261 "It also refers to the quality of the law in question, requiring that it should be accessible to the person concerned, who must moreover be able to foresee its consequences for him, and compatible with the rule of law", Case of Kruslin v. France, Application No. 11801/85.

"Nevertheless, the law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to this secret and potentially dangerous interference with the right to respect for private life and correspondence." Case of Malone v. United Kingdom, Application No. 8691/79.

2262 "The cardinal issue arising under Article 8 (Art. 8) in the present case is whether the interference so found is justified by the terms of paragraph 2 of the Article (Art. 8-2). This paragraph, since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterizing as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions", Case of Klass and others v. Germany, Application No. 5029/71.

2263 "Proportionality shall be implemented by each Party in accordance with relevant principles of its domestic law. For European countries, this will be derived from the principles of the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, its applicable jurisprudence and national legislation and jurisprudence, that the power or procedure shall be proportional to the nature and circumstances of the offence. Other States will apply related principles of their law, such as limitations on overbreadth of production orders and reasonableness requirements for searches and seizures." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

2264 The list is not concluding. See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

2265 "National legislatures will have to determine, in applying binding international obligations and established domestic principles, which of the powers and procedures are sufficiently intrusive in nature to require implementation of particular conditions and safeguards." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 147.

2266 See below: § 6.2.9.

2267 See below: § 6.2.10.

2268 "Also, the explicit limitation in Article 21 that the obligations regarding interception measures are with respect to a range of serious offences, determined by domestic law, is an explicit example of the application of the proportionality principle." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 146.

"Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

"Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 230.

2269 See below: § 6.3.4.

2270 See below: § 6.3.7.

2271 As explained in more detail below, Art. 16 does not oblige the provider to transfer the relevant data to the authorities. It only authorizes the law-enforcement agencies to prevent the deletion of the relevant data. The advantage of separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for their application.

2272 A definition of the term "subscriber information" is provided in Art. 18 Subparagraph 3 of the Convention on Cybercrime.

2273 A definition of the term "computer data" is provided in Art. 1 of the Convention on Cybercrime.

2274 As described more in detail below, the differentiation between "computer data" and "subscriber information" in Art. 18 of the Convention on Cybercrime enables the signatory states to develop graded safeguards with regard to the production order.

2275 "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required", see: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 155. Regarding the identification of suspects by IP-based investigations, see: *Gercke*, Preservation of User Data, DUD 2002, page 577 *et seq.*

2276 *Gercke*, Preservation of User Data, DUD 2002, 578.

2277 The cost issue was especially raised within the discussion on data retention legislation in the EU. See, for example: E-communications service providers remain seriously concerned with the agreement reached by European Union Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005, available at: www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

2278 Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

2279 The discussion already took place at the beginning of 2000. In a G8 Meeting in Tokyo experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding implementation of a data retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report of the Workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001. A similar discussion took place during the negotiation of the Convention on Cybercrime. The drafters explicitly pointed out that the Convention does not establish a data retention obligation. See Explanatory Report to the Convention on Cybercrime, No. 151, available at: http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm.

2280 Regarding The Data Retention Directive in the European Union, see: *Bignami*, Privacy and Law Enforcement in the European Union: The Data Retention Directive, Chicago Journal of International Law, 2007, Vol. 8, No.1, available at: http://eprints.law.duke.edu/archive/00001602/01/8_Chi._J._Int'l_L._233_(2007).pdf; *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq*.

2281 Art. 6 Periods of Retention

Member States shall ensure that the categories of data specified in Article 5 are retained for periods of not less than six months and not more than two years from the date of the communication.

Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

2282 See: Preface 11 of the European Union Data Retention Directive: "Given the importance of traffic and location data for the investigation, detection, and prosecution of criminal offences, as demonstrated by research and the practical experience of several Member States, there is a need to ensure at European level that data that are generated or processed, in the course of the supply of communications services, by providers of publicly available electronic communications services or of a public communications network are retained for a certain period, subject to the conditions provided for in this Directive."

2283 Directive 2002/58/EC of the European Parliament and of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). The document is available at: http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_201/l_20120020731en00370047.pdf.

2284 See, for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes – Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007, available at: www.govtrack.us/congress/bill.xpd?bill=h110-837. Regarding the current situation in the US, see: ABA International Guide to Combating Cybercrime, page 59.

2285 See *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

2286 However, it is recommended that states consider the establishment of powers and procedures to actually order the recipient of the order to preserve the data, as quick action by this person can result in the more expeditious implementation of the preservation measures in particular cases. Explanatory Report to the Convention on Cybercrime, No. 160.

2287 *Gercke*, Cybercrime Training for Judges, 2009, page 63, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2288 See: *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 803.

2289 "Preservation" requires that data which already exists in a stored form be protected from anything that would cause its current quality or condition to change or deteriorate. Explanatory Report to the Convention on Cybercrime, No. 159.

2290 Explanatory Report, No. 152.

2291 Regarding the advantages of a system of graded safeguards, see above: § 6.3.3.

2292 "The reference to 'order or similarly obtain' is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor)". See Explanatory Report to the Convention on Cybercrime, No. 160.

2293 The drafters of the Convention on Cybercrime tried to approach the problems related to the need for immediate action from law-enforcement agencies on the one hand and the importance of ensuring safeguards on the other in a number of ways. Another example for the approach is related to the production order (Art. 18). The drafters suggested that the requirements for the handout of data to law-enforcement agencies could be adjusted in relation to the categories of data. See Explanatory Report to the Convention on Cybercrime, No. 174: "The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

2294 *Gercke*, Cybercrime Training for Judges, 2009, page 64, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2295 An IP address does not necessary immediately identify the offender. If law-enforcement agencies know the IP address an offender used to commit an offence, this information only enables them to identify the connection used to log on to the Internet. If a group of people had access to this connection (e.g. in an Internet café), further investigations are necessary to identify the offender.

2296 If the offender is using services that do not require a registration or if the subscriber information provided by the user is not verified, Art. 18 Subparagraph 1b) will not enable the law-enforcement agencies to immediately identify the offender. Art. 18 Subparagraph 1b) is therefore especially relevant with regard to commercial services (like providing Internet access, commercial e-mail or hosting services).

2297 *Gercke*, The Convention on Cybercrime, Multimedia und Recht 2004, page 802.

2298 "Often, however, no single service provider possesses enough of the crucial traffic data to be able to determine the actual source or destination of the communication. Each possesses one part of the puzzle, and each of these parts needs to be examined in order to identify the source or destination." See Explanatory Report to the Convention on Cybercrime, No. 167.

2299 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2300 Official Note: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.

Official Note: Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

2301 The Commonwealth Model Law contains an alternative provision:

"Sec. 16: If a magistrate is satisfied on the basis of an *ex parte* application by a police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:

(a) the service providers; and

(b) the path through which the communication was transmitted."

2302 For an introduction to data retention, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*; *Blanchette/Johnson*, Data retention and the panoptic society: The social benefits of forgetfulness, available at: http://polaris.gseis.ucla.edu/blanchette/papers/is.pdf.

2303 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

2304 Judgement in Joined Cases C-293/12 and C-594/12.

2305 See, for example: Briefing for the Members of the European Parliament on Data Retention, available at: www.edri.org/docs/retentionletterformeps.pdf; CMBA, Position on Data retention: GILC, Opposition to data retention continues to grow, available at: www.vibe.at/aktionen/200205/data_retention_30may2002.pdf. Regarding the concerns relating to violation of the European Convention on Human Rights, see: *Breyer*, Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR, European Law Journal, 2005, page 365 *et seq.*

2306 See: Heise News, 13 000 determined to file suit against data retention legislation, 17.11.2007, available at: www.heise.de/english/newsticker/news/99161/from/rss09.

2307 Case C-275/06.

2308 See: Advocate General Opinion – 18.07.2007, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62006C0275:EN:NOT#top. The court usually but not invariably follows the adviser's conclusion.

2309 In a G8 meeting in Tokyo, experts discussed the advantages and disadvantages of data retention and data preservation. The experts expressed their concerns regarding an implementation of a data-retention obligation. "Given the complexity of the above noted issues blanket solutions to data retention will likely not be feasible." Report for the workshop on Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers, G8 Government-Industry Workshop on Safety And Security in Cyberspace Tokyo, May 2001.

2310 Regarding the challenges for law-enforcement agencies related to the use of means of anonymous communication, see above: § 3.2.12.

2311 Regarding the technical discussion about traceability and anonymity, see: CERT Research 2006 Annual Report, page 7 *et seq.*, available at: www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

2312 An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2313 See: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 91, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

2314 Regarding the impact of use of anonymous communication technology on the work of law-enforcement agencies, see above: § 3.2.12.

2315 Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2316 Regarding protection of the use of anonymous means of communication by the United States constitution, see: *Aldesco*, The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime, LOLAE Law Review, 2002, page 82, available at: http://elr.lls.edu/issues/v23-issue1/aldesco.pdf.

2317 Judgement in Joined Cases C-293/12 and C-594/12.

2318 A detailed overview of the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq*. For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.* Regarding remote live search and possible difficulties with regard to the principle of chain of custody, see: *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law and Technology Vol. 9, Issue 2, 2005, available at: www.lawtechjournal.com/articles/2005/05_051201_Kenneally.pdf; *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2319 Regarding the involvement of computer forensic experts in investigations, see above: § 6.3.2

2320 Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2321 See below: § 6.3.12.

2322 Apart from the fact that direct access enables the law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

2323 See Explanatory Report to the Convention on Cybercrime, No. 184.

2324 "However, in a number of jurisdictions stored computer data per se will not be considered as a tangible object and therefore cannot be secured on behalf of criminal investigations and proceedings in a parallel manner as tangible objects, other than by securing the data medium upon which it is stored. The aim of Article 19 of this Convention is to establish an equivalent power relating to stored data." Explanatory Report to the Convention on Cybercrime, No. 184. Regarding the special demands with regard to computer-related search and seizure procedures, see: *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2325 Explanatory Report, No. 184.

2326 Regarding the difficulties of online search procedures, see below: § 6.3.12.

2327 See in this context: *Winick*, Search and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, No. 1, page 80.

2328 Regarding the requirements in the US, see for example: *Brenner*, Michigan Telecommunications and Technology Law Review, 2001-2002, Vol. 8, page 41 *et seq.*; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2329 "However, with respect to the search of computer data, additional procedural provisions are necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible data carrier. There are several reasons for this: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record." Explanatory Report to the Convention on Cybercrime, No. 187.

2330 *Gercke*, Cybercrime Training for Judges, 2009, page 69, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079%20if09%20pres%20coe%20train%20manual%20judges6%20_4%20march%2009_.pdf.

2331 *Kerr*, Searches and Seizures in a digital world, Harvard Law Review, 2005, Vol. 119, page 531 *et seq.*

2332 The importance of being able to extend the search to connected computer systems was already addressed by Council of Europe Recommendation No. R (95) 13 of the Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543rd meeting of the Ministers Deputies. The text of the recommendation is available at:

www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf.

2333 In this context, it is important to keep in mind the principle of national sovereignty. If the information is stored on a computer system outside the territory, an extension of the search order could violate this principle. The drafters of the Convention on Cybercrime therefore pointed out: "Paragraph 2 allows the investigating authorities to extend their search or similar access to another computer system or part of it if they have grounds to believe that the data required is stored in that other computer system. The other computer system or part of it must, however, also be in its territory"– Explanatory Report to the Convention on Cybercrime, No. 193. With regard to this issue, see also: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2334 For guidelines how to carry out the seizure of computer equipment, see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory, available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice, available at: www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

2335 Regarding the classification of the act of copying the data, see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 *et seq.*

2336 "Since the measures relate to stored intangible data, additional measures are required by competent authorities to secure the data; that is, 'maintain the integrity of the data', or maintain the 'chain of custody' of the data, meaning that the data which is copied or removed be retained in the State in which they were found at the time of the seizure and remain unchanged during the time of criminal proceedings. The term refers to taking control over or the taking away of data". Explanatory Report to the Convention on Cybercrime, No. 197.

2337 This principle also applies with regard to the seizure of hardware. Compared to maintaining the integrity of copied data it is often easier to maintain the integrity of data on a storage device.

2338 See above: § 2.6.

2339 One possibility to prevent access to the information without deleting it is the use of encryption technology.

2340 See in this context: *Williger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law and Technology, Vol. 10, Issue 5.

2341 The fact that law-enforcement agencies are able to access certain data stored outside the country through a computer system in their territory does not automatically legalize the access. See Explanatory Report to the Convention on Cybercrime, No. 195. "This article does not address 'transborder search and seizure', whereby States could search and seize data in the territory of other States without having to go through the usual channels of mutual legal assistance. This issue is discussed below at the Chapter on international co-operation." Two cases of transborder access to stored computer data are regulated in Art. 32 Convention on Cybercrime:

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

2342 "It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted." Explanatory Report to the Convention on Cybercrime, No. 200.

2343 "A means to order the co-operation of knowledgeable persons would help in making searches more effective and cost efficient, both for law enforcement and innocent individuals affected. Legally compelling a system administrator to assist may also relieve the administrator of any contractual or other obligations not to disclose the data." Explanatory Report to the Convention on Cybercrime, No. 201.

2344 Explanatory Report to the Convention on Cybercrime, No. 202.

2345 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2346 Official Note: If the existing search and seizure provisions contain a description of the content of the warrant, either in a section or by a form, it will be necessary to review those provisions to ensure that they also include any necessary reference to computer data.

2347 Official Note: A country may wish to add a definition of "assist" which could include providing passwords, encryption keys and other information necessary to access a computer. Such a definition would need to be drafted in accordance with its constitutional or common law protections against self-incrimination.

2348 Regarding the motivation of the drafters, see Explanatory Report to the Convention on Cybercrime, No. 171.

2349 "A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability." Explanatory Report to the Convention on Cybercrime, No. 171.

2350 Explanatory Report to the Convention on Cybercrime, No. 173.

2351 "At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement." Explanatory Report to the Convention on Cybercrime, No. 173.

2352 Regarding the possibilities to hinder IP-based investigations by using means of anonymous communication, see above: § 3.2.12.

2353 If the providers offer their service free of charge, they do often either require an identification of the user nor do at least not verify the registration information.

2354 See above: § 6.3.5.

2355 Explanatory Report to the Convention on Cybercrime, No. 172.

2356 This can be, for example, information that was provided on a classic registration form and kept by the provider as paper records.

2357 The Explanatory Report even points out that the parties to the Convention can adjust their safeguards with regard to specific data within each of the categories. See Explanatory Report to the Convention on Cybercrime, No. 174: "Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

2358 For example, the requirement of a court order.

2359 The differentiation between the real-time collection of traffic data (Art. 20) and the real-time collection of content data (Art. 21) shows that the drafters of the Convention realized the importance of separating instruments with different impact.

2360 See below: § 6.3.9.

[2361] See below: § 6.3.10.

[2362] Art. 21 of the Convention on Cybercrime obliges the signatory states to implement the possibility to intercept content data only with regard to serious offences ("Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law"). On the contrary, Art. 20 of the Convention on Cybercrime is not limited to serious offences. "Due to the higher privacy interest associated with content data, the investigative measure is restricted to 'a range of serious offences to be determined by domestic law'." See: Explanatory Report to the Council of Europe Convention on Cybercrime, No. 230.

[2363] Regarding the advantages of a graded system of safeguards, see above: § 6.3.3.

[2364] Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

[2365] Official Note: As noted in the expert group report, in some countries it may be necessary to apply the same standard for production orders as is used for a search warrant because of the nature of the material that may be produced. In other countries it may be sufficient to employ a lower standard because the production process is less invasive than the search process.

Official Note: Countries may wish to consider whether subparagraph c is appropriate for inclusion in domestic law because while it may be of great practical use, it requires the processing and compilation of data by court order, which may not be suitable for some jurisdictions.

[2366] Regarding the legislation on legal interception in Great Britain, Canada, South Africa, United States (New York) and Israel, see: Legal Opinion on Intercept Communication, 2006, available at: www.law.ox.ac.uk/opbp/OPBP%20Intercept%20Evidence%20Report.pdf.

[2367] In these cases, other technical solutions for surveillance need to be evaluated. Regarding possible physical surveillance techniques, see: *Slobogin*, Technologically-assisted physical surveillance: The American Bar Association's Tentative Draft Standards, Harvard Journal of Law & Technology, Vol. 10, Nr. 3, 1997, page 384 *et seq.*

[2368] Regarding the interception of VoIP to assist law-enforcement agencies, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[2369] Regarding the interception of VoIP to assist law-enforcement agencies, see: ITU Global Cybersecurity Agenda/High-Level Experts Group, Global Strategic Report, 2008, page 48, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.htm; *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[2370] In particular, lack of technical preparation of Internet providers to collect the relevant data in real time.

[2371] Explanatory Report to the Convention on Cybercrime, No. 205.

[2372] ABA International Guide to Combating Cybercrime, page 125.

[2373] ABA International Guide to Combating Cybercrime, page 125.

[2374] The "origin" refers to a telephone number, Internet protocol (IP) address or similar identification of a communications facility to which a service provider renders services. Explanatory Report to the Convention on Cybercrime, No. 30.

[2375] "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less

intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive." See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in cybercrime investigations, see also: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 *et seq.*

2376 "In general, the two possibilities for collecting traffic data in paragraph 1(a) and (b) are not alternatives. Except as provided in paragraph 2, a Party must ensure that both measures can be carried out. This is necessary because if a service provider does not have the technical ability to assume the collection or recording of traffic data (1(b)), then a Party must have the possibility for its law enforcement authorities to undertake themselves the task (1(a))." Explanatory Report to the Convention on Cybercrime, No. 223.

2377 The Convention does not define technical standards regarding the design of such an interface. Explanatory Report to the Convention on Cybercrime, No. 220.

2378 Explanatory Report to the Convention on Cybercrime, No. 223.

2379 "The article [Art. 20] does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not require them to acquire or develop new equipment, hire expert support or engage in costly re-configuration of their systems." Explanatory Report to the Convention on Cybercrime, No. 221.

2380 See above: § 3.2.12.

2381 Tor is a software that enables users to protect against traffic analysis. For more information about the software, see: http://tor.eff.org/.

2382 An example of an approach to restrict the use of public terminals to commit criminal offences is Art. 7 of Italian Decree-Law No. 144. The provision forces anybody who intends to offer public Internet access (e.g. Internet cafes) to apply for an authorization. In addition, he is obliged to request an identification from his customers prior to the use of his services. Decree-Law 27 July 2005, No. 144. – Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2383 This advantage is also relevant for remote forensic investigations. See below: § 6.3.12.

2384 Such obligation might be legal or contractual.

2385 Explanatory Report to the Convention on Cybercrime, No. 226.

2386 Regarding the key intention, see Explanatory Report on the Convention on Cybercrime No. 16: "The Convention aims principally at (1) harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime (2) providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form (3) setting up a fast and effective regime of international co-operation."

2387 The drafters of the Convention point out that the signatory states should limit the use of the right to make reservations in this context: Explanatory Report to the Convention on Cybercrime, No. 213.

Regarding the possibilities of making reservations, see Art. 42 Convention on Cybercrime:

Article 42

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No. other reservation may be made.

2388 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at:

www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers,* Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2389 One possibility to prevent law-enforcement agencies from analysing the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures, see: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology, available at: www.cse-cst.gc.ca/documents/about-cse/museum.pdf.

2390 Regarding the impact of encryption technology on computer forensic and criminal investigations, see: *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No. 6, available at: www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf. Regarding legal solutions designed to address this challenge, see below: § 6.3.11.

2391 *Schneier*, Applied Cryptography, page 185.

2392 Model Law on Computer and Computer Related Crime, LMM(02)17; The Model Law is available at: www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf. For more information, see: *Bourne*, 2002 Commonwealth Law Ministers Meeting: Policy Brief, page 9, available at: www.cpsu.org.uk/downloads/2002CLMM.pdf; *Angers*, Combating Cyber-Crime: National Legislation as a pre-requisite to International Cooperation in: *Savona*, Crime and Technology: New Frontiers for Regulation, Law Enforcement and Research, 2004, page 39 *et seq.*; United Nations Conference on Trade and Development, Information Economy Report 2005, UNCTAD/SDTE/ECB/2005/1, 2005, Chapter 6, page 233, available at: www.unctad.org/en/docs/sdteecb20051ch6_en.pdf.

2393 ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

2394 *Schneier*, Applied Cryptography, page 185.

2395 Regarding practical approaches to recover encrypted evidence, see: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at:

2396 The issue is, for example, addressed by Recommendation No. R (95) of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with information, 11 September 1995: "14. Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary" and the G8 in the 1997 Meeting in Denver: "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management, which may allow, consistent with these guidelines. Lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies."

2397 For more information, see: *Koops*, The Crypto Controversy. A Key Conflict in the Information Society, Chapter 5.

2398 The need for such authorization is mentioned, for example, in principle 6 of the 1997 Guidelines for Cryptography Policy: "National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible."

2399 This topic was discussed in the deliberations of the US District Court of New Jersey in the case United States v. Scarfo. The District Court decided that the federal wiretapping law and the Fourth Amendment allow law-enforcement agencies to make use of a software to record keystrokes on a suspect's computer (keylogger) in order to intercept a passphrase to an encrypted file (if the system does not operate while the computer is communicating with other computers). See: www.epic.org/crypto/scarfo/opinion.html.

2400 Export limitations on encryption software capable of processing strong keys are not designed to facilitate the work of law-enforcement agencies in the country. The intention of such regulations is to prevent the availability of the technology outside the country. For detailed information on import and export restrictions with regard to encryption technology, see: http://rechten.uvt.nl/koops/cryptolaw/index.htm.

2401 The limitation of the import of such powerful software is even characterized as "misguided and harsh to the privacy rights of all citizens". See, for example: The Walsh Report – Review of Policy relating to Encryption Technologies 1.1.16 available at: www.efa.org.au/Issues/Crypto/Walsh/walsh.htm.

2402 See: *Lewis*, Encryption Again, available at: www.csis.org/media/csis/pubs/011001_encryption_again.pdf.

2403 The key escrow system was promoted by the United States Government and implemented in France for a period in 1996. For more information, see: Cryptography and Liberty 2000 – An International Survey of Encryption Policy, available at: http://www2.epic.org/reports/crypto2000/overview.html#Heading9.

2404 See: *Diehl*, Crypto Legislation, Datenschutz und Datensicherheit, 2008, page 243 *et seq.*

2405 "To counter, inter alia, the use of strong encryption by terrorists, we have endorsed acceleration of consultations and adoption of the OECD guidelines for cryptography policy and invited all states to develop national policies on encryption, including key, management. which may allow, consistent with these guidelines. lawful government access to prevent and investigate acts of terrorism and to find a mechanism to cooperate internationally in implementing such policies", www.g7.utoronto.ca/summit/1997denver/formin.htm.

2406 See, for example: Antigua and Barbuda, Computer Misuse Bill 2006, Art. 25, available at: www.laws.gov.ag/bills/2006/computer-misuse-bill-2006.pdf; Australia, Cybercrime Act, Art. 12, available at: http://scaleplus.law.gov.au/html/comact/11/6458/pdf/161of2001.pdf; Belgium, Wet van 28 november 2000 inzake informaticacriminaliteit, Art. 9 and Code of Criminal Procedure, Art. 88, available at: http://staatsbladclip.zita.be/staatsblad/wetten/2001/02/03/wet-2001009035.html; France, Loi pour la confiance dans l'économie numérique, Section 4, Art. 37, available at: www.legifrance.gouv.fr/affichTexte.do;jsessionid=B78A2A8ED919529E3B420C082708C031.tpdjo12v_3?cidTexte=JORFTEXT000000801164&dateTexte=20080823; United Kingdom, Regulation of Investigatory Powers Act 2000, Art. 49, available at: www.opsi.gov.uk/acts/acts2000/ukpga_20000023_en_1; India, The Information Technology Act, 2000, Art. 69, available at: www.legalserviceindia.com/cyber/itact.html; Irland, Electronic Commerce Act, 2000, Art. 27, available at: www.irlgov.ie/bills28/acts/2000/a2700.pdf; Malaysia, Communications and Multimedia Act, Section 249, available at: www.msc.com.my/cyberlaws/act_communications.asp; Morocco, Loi relative à l'échange électronique de données juridiques, Chapter III, available at: http://droitmaroc.wordpress.com/2008/01/29/loi-n%C2%B0-53-05-relative-a-lechange-electronique-de-donnees-juridiques-integrale/; Netherlands, Wet op de inlichtingen en veiligheidsdiensten 2002, Art. 89, available at www.legalserviceindia.com/cyber/itact.html; South Africa, Regulation of Interception of Communications and Provisions of Communications-Related Information Act, Art. 21, available at: www.info.gov.za/gazette/acts/2002/a70-02.pdf; Trinidad and Tobago, The Computer Misuse Bill 2000, Art. 16, available at: www.ttcsweb.org/articles/computer-laws/computer-misuse-act-2000/compbill.pdf.

2407 An example can be found in Sec. 69 of the Indian Information Technology Act 2000: "Directions of Controller to a subscriber to extend facilities to decrypt information.(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. (2) The subscriber or any person in-charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information." For more information about the Indian Information Technology Act 2000, see: *Duggal*, India's Information Technology Act 2000, available under: http://unpan1.un.org/intradoc/groups/public/documents/apcity/unpan002090.pdf.

2408 For general information on the Act, see: *Brown/Gladman*, The Regulation of Investigatory Powers Bill – Technically inept: ineffective against criminals while undermining the privacy, safety and security of honest citizens and businesses, available at: www.fipr.org/rip/RIPcountermeasures.htm; *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm; ABA International Guide to Combating Cybercrime, page 32.

2409 For an overview of the regulation, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

2410 Regarding the discussion of protection against self-incrimination under United States law, see for example: *Clemens*, No Computer Exception to the Constitution: The First Amendment Protects Against Compelled Production of an Encrypted Document or Private key, UCLA Journal of Law and Technology, Vol. 8, Issue 1, 2004; *Sergienko*, Self Incrimination and Cryptographic Keys, Richmond Journal of Law & Technology, 1996, available at: www.richmond.edu/jolt/v2i1/sergienko.html; *O'Neil*, Encryption and the First Amendment, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art1.pdf; *Fraser*, The Use of Encrypted, Coded and Secret Communication is an "Ancient Liberty" Protected by the United States Constitution, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art2.pdf; *Park*, Protecting the Core Values of the First Amendment in an age of New Technology: Scientific Expression vs. National Security, Virginia Journal of Law and Technology, Vol. 2, 1997, available at: www.vjolt.net/vol2/issue/vol2_art3.pdf; Hearing before the Subcommittee on the Constitution, Federalism, and Property Rights of the Committee on the Judiciary, United States Senate, 150 Congress, Second Session on Examining the Use of Encryption, available at: www.loc.gov/law/find/hearings/pdf/00139296461.pdf.

Regarding the discussion in Europe on self-incrimination, in particular with regard to the European Convention on Human Rights (ECHR), see: *Moules*, The Privilege against self-incrimination and the real evidence, The Cambridge Law Journal, 66, page 528 *et seq.*; *Mahoney*, The Right to a Fair Trail in Criminal Matters under Art. 6 ECHR, Judicial Studies Institute Journal, 2004, page 107 *et seq.*; *Birdling*, Self-incrimination goes to Strasbourg: O'Halloran and Francis vs. United Kingdom, International Journal of Evidence and Proof, Vol. 12, Issue 1, 2008, page 58 *et seq.*; Commission of the European Communities, Green Paper on the Presumption of Innocence, COM (2006) 174, page 7, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0174:FIN:EN:pdf.

2411 Regarding the situation in the US, see: *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf; *Casey* Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf.

2412 In this context, see also: *Walker*, Encryption, and the Regulation of Investigatory Powers Act 2000, available at: www.bileta.ac.uk/01papers/walker.html.

2413 *Lowman*, The Effect of File and Disk Encryption on Computer Forensics, 2010, available at: http://lowmanio.co.uk/share/The%20Effect%20of%20File%20and%20Disk%20Encryption%20on%20Computer%20Forensics.pdf.

2414 Regarding possibilities to circumvent the obligations, see: *Ward*, Campaigners hit by decryption law, BBC News, 20.11.2007, available at: http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/technology/7102180.stm.

2415 A detailed overview of the elements of search procedures as well as the challenges of carrying them out is provided by the ABA International Guide to Combating Cybercrime, 123 *et seq.* For more information on computer-related search and seizure, see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 *et seq.*; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 *et seq.*

2416 Regarding the threat that the suspect could manipulate or delete evidence and the related obligation to keep information about an ongoing investigation based on Art. 20 confidential, see above: § 6.3.9.

2417 There are disadvantages related to remote investigations. Apart from the fact that direct access enables law-enforcement agencies to examine the physical condition of storage media, physical access to a computer system it is the only way to ensure that the files on the suspect's computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system, see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

2418 Regarding the plans of German law-enforcement agencies to develop a software to remotely access a suspect's computer and perform search procedures, see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security, available at: www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News, available at: www.news.com/8301-10784_3-9769886-7.html.

2419 See: *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encryption Threat, International Journal of Digital Evidence, Vol. 2, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0B0C4A4-9660-B26E-12521C098684EF12.pdf; *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf; *Green*, FBI Magic Lantern reality check, The Register, 03.12.2001, available at: www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.200, available at: www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001, available at: www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; *Abreu*, FBI confirms "Magic Lantern" project exists, 2001, available at: www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

[2420] See: *McCullagh*; FBI remotely installs spyware to trace bomb threat, News.com, 18.07.2007, available at: www.news.com/8301-10784_3-9746451-7.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf; Secret online search warrant: FBI uses CIPAV for the first time, Heise News, 19.07.2007, available at: www.heise-security.co.uk/news/92950.

[2421] Computer and Internet protocol address verifier.

[2422] A copy of the search warrant is available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf. Regarding the result of the search, see: www.politechbot.com/docs/fbi.cipav.sanders.search.warrant.071607.pdf. For more information about CIPAV, see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007, available at: www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV for the first time, Heise Security News, 19.07.2007, available at: www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007, available at: www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008, available at: www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007, available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007, available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.

[2423] Regarding the discussion in Germany, see: The German government is recruiting hackers, Forum for Incident Response and Security Teams, 02.12.2007, available at: www.first.org/newsroom/globalsecurity/179436.html; Germany to bug terrorists' computers, The Sydney Morning Herald, 18.11.2007, available at: www.smh.com.au/news/World/Germany-to-bug-terrorists-computers/2007/11/18/1195321576891.html; *Leyden*, Germany seeks malware "specialists" to bug terrorists, The Register, 21.11.2007, available at: www.theregister.co.uk/2007/11/21/germany_vxer_hire_plan/; Berlin's Trojan, Debate Erupts over Computer Spying, Spiegel Online International, 30.08.2007, available at: www.spiegel.de/international/germany/0,1518,502955,00.html.

[2424] See: Tagesspiegel, Die Ermittler sufen mit, 8.12.2006, available at: www.tagesspiegel.de/politik/;art771,1989104.

[2425] For an overview, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

[2426] The search function was the focus of the decision of the German Supreme Court in 2007. See: Online police searches found illegal in Germany, 14.02.2007, available at: www.edri.org/edrigram/number5.3/online-searches.

[2427] Regarding investigations involving VoIP, see: *Bellovin and others*, Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP, available at www.itaa.org/news/docs/CALEAVOIPreport.pdf; *Simon/Slay*, Voice over IP: Forensic Computing Implications, 2006, available at: http://scissec.scis.ecu.edu.au/wordpress/conference_proceedings/2006/forensics/Simon%20Slay%20-%20Voice%20over%20IP-%20Forensic%20Computing%20Implications.pdf.

[2428] See: *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AF2FB-BD97-C28C-7F9F4349043FD3A9.pdf. Keylogging is the focus of the FBI software "magic lantern". See: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 *et seq.*, available at: http://jolt.law.harvard.edu/articles/pdf/v15/15HarvJLTech521.pdf; Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3, available at: http://assets.opencrs.com/rpts/RL32706_20070926.pdf. See also: ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 49, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[2429] This is the focus of the US investigation software CIPAV. Regarding the functions of the software, see the search warrant, available at: http://blog.wired.com/27bstroke6/files/timberline_affidavit.pdf.

[2430] Regarding these functions, see: *Gercke*, Secret Online Search, Computer und Recht 2007, page 246 *et seq.*

[2431] Regarding the possible ways of infecting a computer system by spyware, see: The spying game: how spyware threatens corporate security, Sophos white paper, 2005, available at: www.cehs.usu.edu/facultyandstaff/security/sophos-spyware-wpus.pdf.

[2432] With regard to the efficiency of virus scanners and protection measures implemented in the operating systems, it is likely that the functioning of a remote forensic software would require the cooperation of software companies. If software companies agree to prevent detection of remote forensic software, this could result in serious risks for computer security. For more information, see: *Gercke*, Computer und Recht 2007, page 249.

2433 If the offender stores illegal content on an external storage device that is not connected to a computer system, the investigators will in general not be able to identify the content if they only have access to the computer system via remote forensic software.

2434 Regarding the importance of maintaining integrity during a forensic investigation, see: *Hosmer*, Providing the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, Vol. 1, Issue 1, available at: www.utica.edu/academic/institutes/ecii/publications/articles/9C4EBC25-B4A3-6584-C38C511467A6B862.pdf; *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, Vol. 1, Issue 2, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A0472DF7-ADC9-7FDE-C80B5E5B306A85C4.pdf.

2435 National sovereignty is a fundamental principle in international law. See: *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

2436 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2437 Explanatory Notes to the Model Legislative Text on Cybercrime, 2010, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2438 See above: § 3.2.12.

2439 Based on Art. 7, "anyone running an establishment open to the public or any kind of private association where devices or terminals, which can be used for electrnic data transmission or other communications, are made available to the public, to customers or members" is obliged to require a licence from local authorities and identify persons using the service. For more information, see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

2440 Decree 144/2005, 27 July 2005 ("Decreto-legge"). Urgent measures for combating international terrorism. For more information about the Decree-Law, see for example the article, Privacy and data retention policies in selected countries, available at www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2026.

2441 For more details, see *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 94 *et seq.*

2442 *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, Computer und Recht International, 2006, page 95.

2443 Regarding the related challenges, see: *Kang*, Wireless Network Security – Yet another hurdle in fighting Cybercrime, in Cybercrime & Security, IIA-2, page 6 *et seq.*

2444 International Mechanisms for Promoting Freedom of Expression, Joint Declaration of the UN Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media and the OAS Special Rapporteur on Freedom of Expression, 2005.

2445 *Büllingen/Gillet/Gries/Hillebrand/Stamm*, Situation and Perspectives of Data Retention in an international comparison (Stand und Perspectiven der Vorratsdatenspeichung im internationalen Vergleich), 2004, page 10, available at: www.bitkom.org/files/documents/Studie_VDS_final_lang.pdf.

2446 *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, Vol. 1, Issue 3, available at: www.utica.edu/academic/institutes/ecii/publications/articles/A04AA07D-D4B8-8B5F-450484589672E1F9.pdf.

2447 Regarding the transnational dimension of cybercrime, see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289, available at: www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension – in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 *et seq.*, available at: http://media.hoover.org/documents/0817999825_1.pdf.

2448 See above: § 3.2.7.

2449 See *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 451 *et seq.*, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page xvii, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2450 See, in this context: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2451 *Gabuardi*, Institutional Framework for International Judicial Cooperation: Opportunities and Challenges for North America, Mexican Law Review, Vol. I, No. 2, page 156, available at: http://info8.juridicas.unam.mx/pdf/mlawrns/cont/2/cmm/cmm7.pdf.

2452 *Gercke*, The Slow Wake of a Global Approach against Cybercrime, Computer Law Review International 2006, 141.

2453 The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

2454 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.PDF.

2455 The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and, the Protocol against the Smuggling of Migrants by Land, Sea and Air and the Protocol Against the Illicit Manufacturing of and Trafficking in Firearms, Their Parts and Components and Ammunition.

2456 Inter-American Convention on Mutual Assistance in Criminal Matters, 1992, Treaty Series, OAS, No. 75. The text of the Convention and a list of signatures and ratifications is available at: www.oas.org/juridico/english/sigs/a-55.html.

2457 European (Council of Europe) Convention on Mutual Assistance in Criminal Matters, 1959, ETS 30.

2458 Council of Europe Convention on Cybercrime, ETS 185.

2459 See in this context the UN Model Treaty on Mutual Legal Assistance, 1999, A/RES/45/117; Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

2460 A full list of agreements is available at: www.ag.gov.au/www/agd/agd.nsf/page/Extradition_and_mutual_assistanceRelationship_with_other_countries.

2461 Second Meeting of Ministers of Justice or of Misters or Attorney General of the American on Cybercrime, Background Documents on the Developments on Cyber Crime in the Framework of the REMJAS and the OAS, 1999, Chapter III, available at: www.oas.org/juridico/english/cybGE_IIIrep3.pdf.

2462 See in this regard: *Pop*, The Principle and General Rules of the International Judicial Cooperation in Criminal Matters, AGORA International Journal of Juridical Science, 2008, page 160 *et seq.*; *Stowell*, International Law: A Restatement of Principles in Conformity with Actual Practice, 1931, page 262; Recueil Des Cours, Collected Courses, Hague Academy of International Law, 1976, page 119.

2463 Convention Against Transnational Organized Crime (2000), GA RES/55/25, Entry into Force: 29.09.2003. Regarding the Convention, see: *Smith*, An International Hit Job: Prosecuting organized Crime Acts as Crimes Against Humanity, Georgetown Law Journal, 2009, Vol. 97, page 1118, available at: www.georgetownlawjournal.org/issues/pdf/97-4/Smith.pdf.

2464 *Choo,* Trends in Organized Crime, 2008, page 273.

2465 *Brenner*, Organized Cybercrime, North Carolina Journal of Law & Technology, 2002, Issue 4, page 27.

2466 See, for example: Great Britain Crown Prosecution Service, Convictions for internet rape plan, Media release, 01.12.2006.

2467 *Choo,* Trends in Organized Crime, 2008, page 273.

2468 For further details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 217, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2469] According to the report of the expert meeting held between 8 and 10 October 2008, there are certain states which require special provisions in their internal law to allow such spontaneous information, while others can transmit information spontaneously without such internal provisions in force: see CTOC/COP/2008/18 page 5.

[2470] For details about the intention of the drafters, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 226, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2471] For details, see: Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime, 2004, page 225, available at: www.unodc.org/pdf/crime/legislative_guides/Legislative%20guides_Full%20version.pdf.

[2472] See, for example, Art. 29 and Art. 35 Convention on Cybercrime.

[2473] The directory is available at: www.unodc.org/compauth/en/index.html. Access requires registration and is reserved for competent national authorities.

[2474] The directory indicates the central authority responsible for receiving the MLA request, languages accepted, channels of communication, contact points, fax and e-mails, specific requests of the receiving states and sometimes even extracts from domestic legislation of that state.

[2475] See CTOC/COP/2008/18, paragraph 27.

[2476] See Art. 25, paragraph 3 of the Convention on Cybercrime.

[2477] The software is available at: www.unodc.org/mla/index.html.

[2478] See Explanatory Report to the Convention on Cybercrime, No. 243. The Member States have the possibility to limit the international cooperation with regard to certain measures (extradition, real time collection of traffic data and the interception of content data).

[2479] If, for example, two countries involved in a cybercrime investigation already have bilateral agreements in place that contain the relevant instruments, those agreements will remain a valid basis for the international cooperation.

[2480] Regarding the difficulties with the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

[2481] The Explanatory Report clarifies that the determination of the covered offences does not depend on the actual penalty imposed in the particular cases. See: Explanatory Report to the Convention on Cybercrime, No. 245.

[2482] Regarding the dual criminality principle, see: *Hafen*, International Extradition: Issues Arising Under the Dual Criminality Requirement, Brigham Young University Law Review, 1992, page 191 *et seq.*, available at: http://lawreview.byu.edu/archives/1992/1/haf.pdf.

[2483] See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[2484] See above: § 3.2.10.

[2485] See Explanatory Report to the Convention on Cybercrime, No. 256.

[2486] This information often leads to successful international investigations. For an overview of large-scale international investigations related to child pornography, see: *Krone*, International Police Operations Against Online Child Pornography, Trends and Issues in Crime and Criminal Justice, No. 296, page 4, available at: www.ecpat.se/upl/files/279.pdf.

[2487] Similar instruments can be found in other Council of Europe conventions. For example, Article 10 of the Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and Article 28 of the Criminal Law Convention on Corruption. Council of Europe conventions are available at: www.coe.int.

[2488] See Explanatory Report to the Convention on Cybercrime, No. 262.

[2489] Regarding the 24/7 network points of contact, see below: § 6.4.12.

[2490] See Explanatory Report to the Convention on Cybercrime, No. 265: "Initially, direct transmission between such authorities is speedier and more efficient than transmission through diplomatic channels. In addition, the establishment of an active central authority serves an important function in ensuring that both incoming and outgoing requests are diligently pursued, that advice is provided to foreign law enforcement partners on how best to satisfy legal requirements in the requested Party, and that particularly urgent or sensitive requests are dealt with properly."

[2491] See Explanatory Report to the Convention on Cybercrime, No. 268.

[2492] See Explanatory Report to the Convention on Cybercrime, No. 269. "Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests), furnishing the specific data sought by the requesting Party would raise difficulties so fundamental as to be considered by the requested Party to fall within the essential interests ground of refusal."

[2493] See Explanatory Report to the Convention on Cybercrime, No. 269.

[2494] See above: § 6.3.

[2495] The most important instruments established by the Convention on Cybercrime are: Expedited preservation of stored computer data (Art. 16), Expedited preservation and partial disclosure of traffic data (Art. 17), Production order (Art. 18), Search and seizure of stored computer data (Art. 19), Real-time collection of traffic data (Art. 20), Interception of content data (Art. 21).

[2496] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2497] An exemption is Art. 32 of the Convention on Cybercrime – See below. Regarding the concerns related to this instrument, see: Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2: " […] Russian Federation (had a positive approach towards the Convention but further consideration would have to be given to Article 32b in particular in the light of experience gained from the use of this Article).

[2498] See above: § 6.3.4.

[2499] See above: § 6.3.4.

[2500] See above: § 6.3.7.

[2501] See above: § 6.3.6.

[2502] See above: § 6.3.9.

[2503] See above: § 6.3.10.

[2504] See Explanatory Report to the Convention on Cybercrime, No. 293.

[2505] "The drafters ultimately determined that it was not yet possible to prepare a comprehensive, legally binding regime regulating this area. In part, this was due to a lack of concrete experience with such situations to date; and, in part, this was due to an understanding that the proper solution often turned on the precise circumstances of the individual case, thereby making it difficult to formulate general rules." See Explanatory Report to the Convention on Cybercrime, No. 293.

[2506] See below in this chapter.

[2507] See Explanatory Report to the Convention on Cybercrime, No. 293.

[2508] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 2.

[2509] See: Challenges and Best Practices in Cybercrime Investigation, 2008, available at: www.unafei.or.jp/english/pdf/PDF_rms/no79/15_P107-112.pdf.

[2510] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2511] For more information, see: A Draft Commentary on the Council of Europe Convention, October 2000, available at: www.privacyinternational.org/issues/cybercrime/coe/analysis22.pdf.

[2512] In this context, it is necessary to point out a difference between Art. 32 and Art. 18. Unlike Art. 18, Art. 32 does not enable a foreign law-enforcement agency to order the submission of the relevant data. It can only seek permission.

[2513] Communiqué of the Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, Moscow, 19-20 October 1999.

[2514] Principles on Transborder Access to Stored Computer Data, available at: www.justice.gov/criminal/cybercrime/g82004/99TransborderAccessPrinciples.pdf.

[2515] The need to speed up the process of international cooperation is pointed out in the Explanatory Report. See Explanatory Report to the Convention on Cybercrime, No. 256: "Computer data is highly volatile. By a few keystrokes or by operation of automatic programs, it may be deleted, rendering it impossible to trace a crime to its perpetrator or destroying critical proof of guilt. Some forms of computer data are stored for only short periods of time before being deleted. In other cases, significant harm to persons or property may take place if evidence is not gathered rapidly. In such urgent cases, not only the request, but the response as well should be made in an expedited manner. The objective of Paragraph 3 is therefore to facilitate acceleration of the process of obtaining mutual assistance so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to."

[2516] See above: § 6.3.4.

[2517] Availability 24 hours a day and 7 days a week is especially important with regard to the international dimension of cybercrime, as requests can potentially come from any time zone in the world. Regarding the international dimension of cybercrime and the related challenges, see above: § 3.2.6.

[2518] See Explanatory Report to the Convention on Cybercrime, No. 298.

[2519] Regarding the activities of the G8 in the fight against cybercrime, see above: § 5.1.1. For more information on the 24/7 Network, see: *Sussmann*, The Critical Challenges from International High-Tech and Computer-related Crime at the Millennium, Duke Journal of Comparative & International Law, 1999, Vol. 9, page 484, available at: www.g7.utoronto.ca/scholar/sussmann/duke_article_pdf.

[2520] See above: § 3.2.10.

[2521] See above: § 3.2.6.

[2522] Regarding the question of which authorities should be authorized to order the preservation of data, see above: § 6.3.4.

[2523] Explanatory Report to the Convention on Cybercrime, No. 301.

[2524] Report of the 2nd Meeting of the Cybercrime Convention Committee, T-CY (2007) 03, page 5 (35).

[2525] *Verdelho*, The effectiveness of international cooperation against cybercrime, 2008, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/567%20study4-Version7%20provisional%20_12%20March%2008_.pdf.

[2526] The Functioning of 24/7 points of contact for cybercrime, 2009, available at: www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Points%20of%20Contact/567_24_7report3a%20_2%20april09.pdf.

[2527] The Stanford Draft International Convention was developed as a follow-up to a conference hosted in Stanford University in the US in 1999. The text of the Convention is published in: The Transnational Dimension of Cyber Crime and Terror, page 249 *et seq.*, available at: http://media.hoover.org/documents/0817999825_249.pdf. For more information, see: *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, UCLA Journal of Law and Technology, Vol. 6, Issue 1, 2002, page 70, available at: www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Sofaer,* Toward an International Convention on Cyber in *Seymour/Goodman*, The Transnational Dimension of Cyber Crime and Terror, page 225, available at: http://media.hoover.org/documents/0817999825_221.pdf; ABA International Guide to Combating Cybercrime, 2002, page 78.

[2528] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[2529] See *Sofaer/Goodman/Cuellar/Drozdova and others*, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000, available at: www.iwar.org.uk/law/resources/cybercrime/stanford/cisac-draft.htm.

[2530] Regarding the network architecture and the consequences with regard to the involvement of service providers, see: *Black*, Internet Architecture: An Introduction to IP Protocols, 2000; *Zuckerman/McLaughlin*, Introduction to Internet Architecture and Institutions, 2003, available at: http://cyber.law.harvard.edu/digitaldemocracy/internetarchitecture.html.

[2531] See in this context: *Sellers*, Legal Update to: Shifting the Burden to Internet Service Providers: The Validity of Subpoena Power under the Digital Millennium Copyright Act, Oklahoma Journal of Law and Technology, 8a, 2004, available at: www.okjolt.org/pdf/2004okjoltrev8a.pdf.

[2532] National sovereignty is a fundamental principle in international law. See *Roth*, State Sovereignty, International Legality, and Moral Disagreement, 2005, page 1, available at: www.law.uga.edu/intl/roth.pdf.

[2533] For an introduction to the discussion, see: *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.,* available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

[2534] In the decision Recording Industry Association Of America v. Charter Communications, Inc., the United States Court of Appeals for the eighth circuit described (by referring to House Report No. 105-551(II) at 23 (1998)) the function of the United States DMCA by pointing out the balance. In the opinion of the court, DMCA has "two important priorities: promoting the continued growth and development of electronic commerce and protecting intellectual property rights."

[2535] Regarding the history of DMCA and pre-DMCA case law in the United States, see: *Ciske*, For Now, ISPs must stand and deliver: An analysis of In re Recording Industry Association of America vs. Verizon Internet Services, Virginia Journal of Law and Technology, Vol. 8, 2003, available at: www.vjolt.net/vol8/issue2/v8i2_a09-Ciske.pdf; *Salow*, Liability Immunity for Internet Service Providers – How is it working?, Journal of Technology Law and Policy, Vol. 6, Issue 1, 2001, available at: http://grove.ufl.edu/~techlaw/vol6/issue1/pearlman.html.

[2536] Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf; *Schwartz*, Thinking outside the Pandora's box: Why the DMCA is unconstitutional under Article I, § 8 of the United States Constitution, Journal of Technology Law and Policy, Vol. 10, Issue 1, available at: http://grove.ufl.edu/~techlaw/vol10/issue1/schwartz.html.

[2537] Regarding the application of DMCA to search engines, see: *Walker*, Application of the DMCA Safe Harbor Provisions to Search Engines, Virginia Journal of Law and Technology, Vol. 9, 2004, available at: www.vjolt.net/vol9/issue1/v9i1_a02-Walker.pdf.

[2538] 17 USC. § 512(a).

[2539] 17 USC. § 512(b).

[2540] Regarding the Communications Decency Act, see: *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf;

[2541] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') – Official Journal L 178, 17/07/2000 P. 0001 – 0016. For a comparative law analysis of the United States and European Union e-commerce regulations (including the EU E-Commerce Directive), see: *Pappas*, Comparative US & EU Approaches To E-Commerce Regulation: Jurisdiction, Electronic Contracts, Electronic Signatures And Taxation, Denver Journal of International Law and Policy, Vol. 31, 2003, page 325 *et seq.*, available at: www.law.du.edu/ilj/online_issues_folder/pappas.7.15.03.pdf.

[2542] See *Lindholm/Maennel*, Computer Law Review International 2000, 65.

[2543] Art. 12 – Art. 15 EU of the E-Commerce Directive.

[2544] With the number of different services covered, the E-Commerce Directive aims for a broader regulation than 17 USC. § 517(a). Regarding 17 USC. § 517(a).

[2545] See Art. 12 paragraph 3 of the E-Commerce Directive.

[2546] The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public

Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2547 Regarding traditional caching as well as active caching, see: *Naumenko*, Benefits of Active Caching in the WWW, available at: www.epfl.ch/Publications/Naumenko/Naumenko99.pdf.

2548 For more information on proxy servers, see: *Luotonen*, Web Proxy Servers, 1997.

2549 The provision was implemented by DMCA (Digital Millennium Copyright Act). Regarding the impact of DMCA on the liability of Internet service providers, see: *Unni*, Internet Service Provider's Liability for Copyright Infringement – How to Clear the Misty Indian Perspective, 8 RICH. J.L. & TECH. 13, 2001, available at: www.richmond.edu/jolt/v8i2/article1.html; *Manekshaw*, Liability of ISPs: Immunity from Liability under the Digital Millennium Copyright Act and the Communications Decency Act, Computer Law Review and Technology Journal, Vol. 10, 2005, page 101 *et seq.*, available at: www.smu.edu/csr/articles/2005/Fall/SMC103.pdf; *Elkin-Koren*, Making Technology Visible: Liability of Internet Service Providers for Peer-to-Peer Traffic, Journal of Legislation and Public Policy, Volume 9, 2005, page 15 *et seq.*, available at www.law.nyu.edu/journals/legislation/articles/current_issue/NYL102.pdf.

2550 See above: § 6.5.4.

2551 Regarding the impact of free webspace on criminal investigations, see: *Evers*, Blogging sites harbouring cybercriminals, CNET News, 26.07.2005, available at: http://news.zdnet.co.uk/security/0,1000000189,39210633,00.htm.

2552 This procedure is called "notice and takedown".

2553 The hosting provider is quite often in a difficult situation. On the one hand, it needs to react immediately to avoid liability; on the other hand, it has certain obligations to its customers. If it removes legal information that was just at first sight illegal, this could lead to claims for indemnity.

2554 By enabling their customers to offer products, they provide the necessary storage capacity for the required information.

2555 The Project on Enhancing Competiveness in the Caribbean through the Harmonization of ICT Policies, Legislation and Regulatory Procedures (HIPCAR) is a project conceived by ITU, CARICOM and CTU. Further information is available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2556 See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2557 See the Explanatory Note to the HIPCAR cybercrime model legislative text available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html.

2558 *Spindler*, Multimedia und Recht 1999, page 204.

2559 Art. 21 – Re-examination

1. Before 17 July 2003, and thereafter every two years, the Commission shall submit to the European Parliament, the Council and the Economic and Social Committee a report on the application of this Directive, accompanied, where necessary, by proposals for adapting it to legal, technical and economic developments in the field of information society services, in particular with respect to crime prevention, the protection of minors, consumer protection and to the proper functioning of the internal market.

2. In examining the need for an adaptation of this Directive, the report shall in particular analyse the need for proposals concerning the liability of providers of hyperlinks and location tool services, 'notice and take down' procedures and the attribution of liability following the taking down of content. The report shall also analyse the need for additional conditions for the exemption from liability, provided for in Articles 12 and 13, in the light of technical developments, and the possibility of applying the internal market principles to unsolicited commercial communications by electronic mail.

2560 *Freytag*, Computer und Recht 2000, page 604; *Spindler*, Multimedia und Recht 2002, page 497.

2561 Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

2562 See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

2563 § 17 – Ausschluss der Verantwortlichkeit bei Links

(1) Ein Diensteanbieter, der mittels eines elektronischen Verweises einen Zugang zu fremden Informationen eröffnet, ist für diese Informationen nicht verantwortlich, sofern er von einer rechtswidrigen Tätigkeit oder Information keine tatsächliche Kenntnis hat und sich in Bezug auf Schadenersatzansprüche auch keiner Tatsachen oder Umstände bewusst ist, aus denen eine rechtswidrige Tätigkeit oder Information offensichtlich wird, oder, sobald er diese Kenntnis oder dieses Bewusstsein erlangt hat, unverzüglich tätig wird, um den elektronischen Verweis zu entfernen.

2564 *Introna/Nissenbaum*, Sharping the Web: Why the politics of search engines matters, page 5, available at: www.nyu.edu/projects/nissenbaum/papers/searchengines.pdf.

2565 Austria, Spain and Portugal. See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 7.

2566 See Report of the application of the Directive on electronic commerce – COM (2003) 702, page 15.

2567 Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE) – Artículo 17. Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda (Spain)

1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que: a) No. tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o b) si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere la letra a) cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.

2. La exención de responsabilidad establecida en el apartado primero no operará en el supuesto de que el destinatario del servicio actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos.

2568 Ausschluss der Verantwortlichkeit bei Suchmaschinen

§ 14. (1) Ein Diensteanbieter, der Nutzern eine Suchmaschine oder andere elektronische Hilfsmittel zur Suche nach fremden Informationen bereitstellt, ist für die abgefragten Informationen nicht verantwortlich, sofern er

1. die Übermittlung der abgefragten Informationen nicht veranlasst,
2. den Empfänger der abgefragten Informationen nicht auswählt und
3. die abgefragten Informationen weder auswählt noch verändert.

(2) Abs. 1 ist nicht anzuwenden, wenn die Person, von der die abgefragten Informationen stammen, dem Diensteanbieter untersteht oder von ihm beaufsichtigt wird.

国际电信联盟（ITU）
电信发展局（BDT）
主任办公室
Place des Nations
CH-1211 Geneva 20 – Switzerland
电子邮件： bdtdirector@itu.int
电话： +41 22 730 5035/5435
传真： +41 22 730 5484

副主任
兼行政和运营协调部负责人（DDR）
电子邮件： bdtdeputydir@itu.int
电话： +41 22 730 5784
传真： +41 22 730 5484

基础设施、环境建设和
电子应用部（IEE）
电子邮件： bdtiee@itu.int
电话： +41 22 730 5421
传真： +41 22 730 5484

创新和
合作伙伴部（IP）
电子邮件： bdtip@itu.int
电话： +41 22 730 5900
传真： +41 22 730 5484

项目支持和
知识管理部（PKM）
电子邮件： bdtpkm@itu.int
电话： +41 22 730 5447
传真： +41 22 730 5484

非洲

埃塞俄比亚
国际电联
区域代表处
P.O. Box 60 005
Gambia Rd., Leghar ETC Building
3rd floor
Addis Ababa – Ethiopia

电子邮件： itu-addis@itu.int
电话： +251 11 551 4977
电话： +251 11 551 4855
电话： +251 11 551 8328
传真： +251 11 551 7299

喀麦隆
国际电联
地区办事处
Immeuble CAMPOST, 3e étage
Boulevard du 20 mai
Boîte postale 11017
Yaoundé – Cameroon

电子邮件： itu-yaounde@itu.int
电话： + 237 22 22 9292
电话： + 237 22 22 9291
传真： + 237 22 22 9297

塞内加尔
国际电联
地区办事处
19, Rue Parchappe x Amadou
Assane Ndoye
Immeuble Fayçal, 4e étage
B.P. 50202 Dakar RP
Dakar – Sénégal

电子邮件： itu-dakar@itu.int
电话： +221 33 849 7720
传真： +221 33 822 8013

津巴布韦
国际电联
地区办事处
TelOne Centre for Learning
Corner Samora Machel and
Hampton Road
P.O. Box BE 792 Belvedere
Harare – Zimbabwe

电子邮件： itu-harare@itu.int
电话： +263 4 77 5939
电话： +263 4 77 5941
传真： +263 4 77 1257

美洲

巴西
国际电联
区域代表处
SAUS Quadra 06, Bloco “E”
11° andar, Ala Sul
Ed. Luis Eduardo Magalhães (Anatel)
70070-940 Brasilia, DF – Brazil

电子邮件： itubrasilia@itu.int
电话： +55 61 2312 2730-1
电话： +55 61 2312 2733-5
传真： +55 61 2312 2738

巴巴多斯
国际电联
地区办事处
United Nations House
Marine Gardens
Hastings, Christ Church
P.O. Box 1047
Bridgetown – Barbados

电子邮件： itubridgetown@itu.int
电话： +1 246 431 0343/4
传真： +1 246 437 7403

智利
国际电联
地区办事处
Merced 753, Piso 4
Casilla 50484, Plaza de Armas
Santiago de Chile – Chile

电子邮件： itusantiago@itu.int
电话： +56 2 632 6134/6147
传真： +56 2 632 6154

洪都拉斯
国际电联
地区办事处
Colonia Palmira, Avenida Brasil
Ed. COMTELCA/UIT, 4.º piso
P.O. Box 976
Tegucigalpa – Honduras

电子邮件： ituteguciglapa@itu.int
电话： +504 22 201 074
传真： +504 22 201 075

阿拉伯国家

埃及
国际电联
区域代表处
Smart Village, Building B 147, 3rd floor
Km 28 Cairo – Alexandria Desert Road
Giza Governorate
Cairo – Egypt

电子邮件： itucairo@itu.int
电话： +202 3537 1777
传真： +202 3537 1888

亚太

泰国
国际电联
区域代表处
Thailand Post Training Center, 5th floor,
111 Chaengwattana Road, Laksi
Bangkok 10210 – Thailand

邮寄地址：
P.O. Box 178, Laksi Post Office
Laksi, Bangkok 10210 – Thailand

电子邮件： itubangkok@itu.int
电话： +66 2 575 0055
传真： +66 2 575 3507

印度尼西亚
国际电联
地区办事处
Sapta Pesona Building, 13th floor
Jl. Merdan Merdeka Barat No. 17
Jakarta 10001 – Indonesia

邮寄地址：
c/o UNDP – P.O. Box 2338
Jakarta 10001 – Indonesia

电子邮件： itujakarta@itu.int
电话： +62 21 381 3572
电话： +62 21 380 2322
电话： +62 21 380 2324
传真： +62 21 389 05521

独联体国家

俄罗斯联邦
国际电联
地区办事处
4, Building 1
Sergiy Radonezhsky Str.
Moscow 105120
Russian Federation

邮寄地址：
P.O. Box 25 – Moscow 105120
Russian Federation

电子邮件： itumoskow@itu.int
电话： +7 495 926 6070
传真： +7 495 926 6073

欧洲

瑞士
国际电联
电信发展局（BDT）欧洲处（EUR）
Place des Nations
CH-1211 Geneva 20 – Switzerland
Switzerland
电子邮件： eurregion@itu.int
电话： +41 22 730 5111

国际电信联盟
电信发展局
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

ISBN 978-92-61-15645-9 SAP id 39681

瑞士印刷
2014年，日内瓦
图片鸣谢：Shutterstock

11/2014