VISITING EXPERTS' PAPERS

AN INTRODUCTION TO CYBERCRIME

*Marco Gercke**

I. THE IMPORTANCE OF THE ABILITY TO FIGHT CYBERCRIME

A. Development towards an Information Society

The development of the Internet and its continuing growth has a significant impact on the development of societies worldwide.[1] Developing countries as well as developed countries have started to turn into information societies.[2] The process is in general characterized by an emerging use of information technology to access and share information.[3] It offers various opportunities that range from access to information to the ability to communicate with any user who has access to the Internet.[4] These advantages led to an ongoing process of integrating information technology into the everyday life of people worldwide.[5] More than a billion people are already using the Internet.[6] Not only individuals but also businesses benefit from the emerging use of the Internet. They can offer goods and services in a global environment with very little financial investment.[7]

B. Importance of the Ability to Fight Cybercrime

The ability to effectively fight against cybercrime is an essential requirement to support the initiation and continuation of this process.[8] Without creating the legal framework that enables law enforcement agencies to identify offenders and prosecute them, it is almost impossible to stop such cybercrime attacks. Despite the importance of technical protection measures[9] in the prevention of cybercrime it is important to highlight, that especially in those cases, where such technology is not available, failed, or was circumvented the existence of a proper legal framework is of great importance for recreating and maintaining cyber-security.

---

* Professor, University of Cologne, Germany. This article is an excerpt from a publication that the author drafted for the Council of Europe. The author would like to thank the Council of Europe for the permission to use the publication as a contribution to this publication.

[1] Related to the development of the Internet, see: *Yang, Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, Page 52 – 56.

[2] 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.

[3] World Summit on the Information Society, Document WSIS-03/GENEVA/DOC/5-E, December 2003, available at: http://www.itu.int/wsis/docs/geneva/official/poa.html

[4] 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.

[5] 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. 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.

[6] According to the ITU, there were 1.14 billion Internet users by the start of 2007, available at: http://www.itu.int/ITU-D/icteye.default.asp.

[7] See for example: Impact of the IT Revolution on the Economy and Finance, Report from G7 Finance Ministers to the Heads of State and Government, 2000 – available at: http://www.mof.go.jp/english/if/if020.pdf.

[8] Regarding the importance of the availability of a legal framework to effectively fight Cybercrime see *Gercke*, The slow wake of a global approach against Cybercrime, CRi 2006, page 140 et seqq.

[9] See for example US GAO, Technology Assessment, Cybersecurity for Critical Infrastructure Protection, GAO Document GAO-04-321, page 44 et seqq. – available at: http://www.gao.gov/new.items/d04321.pdf.

The importance of the ability to ensure that a legal framework for cybercrime investigation and prosecution exists is not limited to direct measures to identify and prosecute offenders. Creating and efficiently using such a legal framework can enhance the trust of individual users as well as businesses in the security of information technology. If users are losing trust in information technology this can negatively influence the development of e-commerce in the affected countries.[10] The existence of a sufficient legal framework for the fight against cybercrime can therefore be considered one essential requirement for e-commerce.[11]

C. Worldwide Phenomenon

The decreasing prices of communication services is one of the reasons why the above mentioned development towards an information society is not limited to the highly developed countries. Developing countries are actively participating in this process.[12] Since 2005 the number of Internet users in developing countries has surpassed the number of users in developed countries.[13] Efforts to enhance cyber-security in those countries where important communication infrastructure (such as servers of search engines or e-mail providers) is located are an important step towards cyber-security.[14] But without the protection of the growing number of users, cyber-security cannot be achieved. The user, from an offender's point of view, is often the weakest point, and needs to be included in the strategy. Phenomena like botnets,[15] which are based on successful mass scale attacks against users, clearly show the importance of the ability to effectively fight against cybercrime in order to protect the users in those countries where Internet users are most numerous.

D. National Interaction and International Co-operation

The fight against cybercrime is proceeding with unique challenges.[16] Two aspects that are of great importance for the success of cybercrime-related investigations are the interaction of the different organizations/institutions on the national level and international co-operation on the global level.

1. Requirements at the National Level

The investigation of cybercrime on a national level can in general only be carried out if the victim, the organizations involved in the fight against cybercrime and the businesses whose services were used are working together closely.

- A first important step is the report of an offence by the victim. Very often the victims of cybercrime do not report offences to the law enforcement agencies.[17] There are two main reasons for this phenomenon. The first reason is the fact that a number of cybercrime scams are based on the principle of multiple offences with a rather small profit each instead of single offences with a high profit. If the damage caused by a single cybercrime is below a certain amount the victims will – after evaluating the time and energy required to report and offence and provide the necessary evidence

[10] *Ratnasingham*, The importance of trust in electronic communication, Internet Research, 1998, Vol. 8, Issue 4, page 313 et. Seqq; *Meech/Marsh*, Social Factors in E-Commerce Personalization – available at: http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-43664.pdf; *Shim/Van Slyke/Jiang/Johnson*, Does Trust reduce concerns for information privacy in e-commerce? – available at: http://sais.aisnet.org/2004/.%5CShim,%20VanSlyke,%20Jiang%20&%20Johnson.pdf.

[11] Regarding the importance of the availability of a legal framework to effectively fight Cybercrime see *Gercke*, The slow wake of a global approach against Cybercrime, CRi 2006, page 140 et seqq.

[12] UK Parlamentary Office of Science and Technology, Postnote, March 2006, No. 261, ICT in Developing Countries; *Nulens*, Digital Divide in Developing Countries: An Information Society in Africa, 2002; *Roy*, Globalisation, ICT and Developing Nations: Challenges in the Information Age, 2005.

[13] See "Development Gateway's Special Report, Information Society – Next Steps?", 2005, available at: http://topics.developmentgateway.org/special/informationsociety.

[14] Regarding the impact of the Council of Europe Convention on Cybercrime on the protection of infrastructure see *Gercke*, National, Regional and International Legal Approaches in the Fight Against Cybercrime, CRi 2008, page 9.

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

[16] See below, section II.

[17] US GAO, Cybercrime – Public and Private Enterties face challenges in addressing cyber threats, GAO document: GAO-07-705 – available at: http://www.gao.gov/new.items/d07705.pdf; Computer Crime & Abuse Report (India) 2001-02, Page 8 – available at: http://www.asianlaws.org/report0102.pdf; *Gross*, Investigator: Report Cybercrime, Info World 2006 – available at: http://www.infoworld.com/archives/emailPrint.jsp?R=printThis&A=/article/06/08/24/HNreportcybercrime_1.html.

with the chance that the offender is identified – decide not to report the offence. But it is not only private users who very often do not report offences. In 2007 the FBI called for business in the US to more intensively report cybercrime.[18] The effect of the underreporting of cybercrime was also addressed by the US Attorney General Ashcroft in 2001. He expressed the opinion that without such reports offenders will go unpunished.[19] In addition, he pointed out that the fear of bad publicity[20] is one of the main reasons why businesses do not report successful cybercrime attacks.[21]

- The second requirement is the ability of the law enforcement agencies to carry out the investigation after an incident was reported by the victim. If they do not have access to the necessary technology, did not receive the required special training or cannot base their work on a legal framework that enables them to carry out the necessary investigations they will very likely not be able to identify the offender.[22]

- In addition, efficient interaction between law enforcement agencies and the judiciary is necessary.[23] One example of the need for co-operation is the court order. In a number of countries certain investigations require a court order.[24] An inefficient interaction between law enforcement and the courts can delay investigations and as a consequence decrease the changes to identify and prosecute the offender.

- Finally cybercrime investigations do very often require access to certain data that is not under control of the law enforcement agencies but in the possession of private businesses such as Internet Service Providers (ISP).[25] Without the assistance of Internet Service Providers investigations can be very time consuming. A legal framework and related procedures that enable efficient co-operation between law enforcement agencies and Internet Service Providers can significantly increase the abilities of the law enforcement agencies to carry out investigations.[26]

2. Requirements at the International Level

Cybercrime is a truly international phenomenon.[27] Due to the structure of the network an offender

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

[19] See Remarks Of Attorney General John Ashcroft at the First Annual Computer Privacy, Policy & Security Institute, 2001 – available at: http://www.justice.gov/criminal/cybercrime/AGCPPSI.htm.

[20] Bases on the Computer Crime & Abuse Report (India) 2001-02 60% of the victims did not report incidents due to fear of bad publicity. See Computer Crime & Abuse Report (India) 2001-02, Page 8 – available at: http://www.asianlaws.org/report0102.pdf.

[21] Not only bad publicity, but also fear of the consequences of freedom of information legislation that could give competitors access to that information.

[22] Regarding training activities in the OAS and the APEC see for example: Cybercrime Convention Committee document T-CY (2006) 6 – available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/(T-CY%20_2006_%2006%20-%20e%20-%20US%20Activities%20to%20ipmrove%20cybercrime%20l_205)_en.pdf; Regarding the importance of the enforcement see *Broadhurst*, Development in the global legal enforcement of cyber-crime, *Policing: An International Journal of Police Strategies and Management* 29, page 408-433.

[23] See: 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 – available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF; *De Hert/Fuster/Koops*, Fighting Cybercrime in the two Europes. The added value of the EU Framework Decision and the Council of Europe Convention, Revue Internationale De Droit Penal, 2006, Vol 77, page 503 et. Seqq.

[24] Regarding the requirement of court orders for certain investigations see the Explanatory Report to the Convention on Cybercrime, Nr. 174.

[25] See: *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime, 2008

[26] See in this context: Guidelines for the cooperation between law enforcement and internet service providers against cybercrime – available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf; Regarding the guidelines see: *Kirk*, Council of Europe, ISPs Draft Anti-Cybercrime Guide, PC World, 01.04.2008, available at: http://www.pcworld.com/businesscenter/article/144011/council_of_europe_isps_draft_anticybercrime_guide.html; *Gercke*, The Council of Europe Guidelines on the Cooperation of ISP and LEA, CRi 2008, issue 4.

[27] Regarding the international dimension of Cybercrime see: *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", CRI 2006, 142.

can act from any place in the world and attack victims worldwide. The ability of national law enforcement agencies to investigate those crimes that have an international dimension is limited due to the principle of national sovereignty that restricts the authorization to carry out investigation in foreign territories.[28] International investigations therefore require co-operation of the law enforcement agencies based on the legal frameworks for international co-operation.[29] The related formal requirements and time needed to collaborate with foreign law enforcement agencies often hinders international investigations.[30]

E. Co-operation between Law Enforcement Agencies and Private Businesses

An effective fight against cybercrime depends not only on the availability of a sufficient legislation – the relationship between the law enforcement agencies and private businesses (such as Internet Service Provider) is considered another essential element.[31] As a result the Council of Europe decided in 2007 to develop a set of guidelines to improve the co-operation between law enforcement agencies and Internet Service Providers.[32] The guidelines were based on a study that analyses the existing structure of co-operation.[33] During the 2008 Council of Europe Octopus Interface Conference[34] the guidelines were adopted.[35] During the meeting of the Cybercrime Committee (T-CY) the committee highlighted the importance of the new guidelines within approaches to promote co-operation.[36]

F. Balancing Freedom of Expression and the Need for Effective Criminal Investigations

The freedom of speech[37] and data protection are two issues that are in the focus of the discussion about the protection of Internet users.[38] In addition to those measures, the prevention of cybercrime and the ability of law enforcement agencies to identify offenders and hinder them from committing further offences enhances cyber-security and thereby increases the security of the user. But in this context it is important

---

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

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

[30] See *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", CRI 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;

[31] See Guidelines for the cooperation of law enforcement and internet service providers against cybercrime, No.3.

[32] For more details see: *Gercke*, The Council of Europe Guidelines for the Cooperation between LEAs and ISP against Cybercrime, Cri 2008, issue 4.

[33] *Callanan/Gercke*, Study on the Cooperation between service providers and law enforcement against cybercrime - Toward common best-of-breed guidelines?, 2008.

[34] The programme of the conference is available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567%20IF08-m-programme3b%20Provisional%20%20(26%20march%2008).PDF. The conclusions of the conference is available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_IF08-d-concl1c.pdf.

[35] Guidelines for the co-operation between law enforcement and internet service providers against cybercrime - available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_prov-d-guidelines_provisional2_3April2008_en.pdf.

[36] The Cybercrime Convention Committee (T-CY), 3rd Consultations of the Parties to the Convention on Cybercrime (ETS No. 185), Meeting Report, 2008, No. 42 - available at: http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/T-CY/T-CY_2008(04)-Final_en.pdf.

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

[38] Regarding the fundamental rights of the users that need to be protected see for example: World Summit of the Information Society, Declaration of Principles, 2003 - http://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

to highlight that some of the measures designed to increase the ability of law enforcement agencies to investigate cybercrime that are currently discussed (such as data retention obligations) raise concerns that the measures do interfere with the fundamental rights of the users.[39] Balancing the necessity of effective instruments for cybercrime-related investigations and the protection of fundamental rights of the user is therefore an important aspect that needs to be taken into consideration while implementing legal frameworks as well as their application within the investigation.

II. THE CHALLENGE IN FIGHTING CYBERCRIME

The Internet is still one of the fastest growing areas of technical infrastructure development.[40] Within this development, it has grown at an enormous rate since the introduction of the World Wide Web's graphical user interface in the 1990. The process of the introduction of Internet Communication Services into everyday life turns out to be so extensive that it appears to be adequate to speak about a trend towards an Information Society. For society, this development goes along with great opportunities. As examples from Eastern Europe show, the unfiltered access to information can support democracy as the flow of information is taken out of the control of state authorities. The improvement is not limited to these general developments. Law enforcement agencies benefit from the increasing power of computer systems as well. They are today able to automatically carry out investigations that were not possible in the past. An example is the automatic search for evidence on a suspect's computer. Modern forensic systems are able to carry out a hash-values-based search for child pornography pictures as well as for keywords in text documents.

But the integration of information technology is accompanied by serious threats as well. In a society where nearly all services depend on the availability of information technology, attacks against this infrastructure have great risks.[41] In addition, offenders can make use of information technology to protect their criminal activities against a discovery by law enforcement agencies. If the offenders for example encrypt child pornography images stored on their computer the automatic search functions of forensic tools will not be able to identify them. The following chapter gives an overview of some of the most important challenges that law enforcement agencies face while investigating and prosecuting cybercrime cases.

A. Dependence of Society on Information Technology

The modern societies are already heavily dependent on the availability of information technology, such as Internet phone calls or e-mail communication,[42] and the integration of the communication technology is still continuing.[43] This development attracts threats of attack against critical infrastructures such as electricity supply and communication infrastructure.[44] Even short interruptions of these services have the potential to cause huge financial damage to e-commerce dependant businesses.

From a cyber-security perspective this development is risky as the existing technical infrastructure shows a number of weak points, such as the monoculture of operating systems.[45] The monoculture offers a

---

[39] Regarding the concerns see for example: Memorandum of Laws Concerning the Legality of Data Retention with regard to the rights guaranteed by the European Convention on Human Rights, 2003 – available at: http://www.privacyinternational.org/countries/uk/surveillance/pi_data_retention_memo.pdf.

[40] Related to the development of the Internet see: *Yang*, *Miao*, ACM International Conference Proceeding Series; Vol. 113; Proceedings of the 7th International Conference on Electronic Commerce, Page 52 – 56; According to "Internet World Stats" about one billion people were using the Internet by 2006 (the statistics are available at: http://www.internetworldstats.com/stats.htm - March 2006).

[41] Related to Cyberterrorism see: *Sofaer*, The Transnational Dimension of Cybercrime and Terrorism, Page 221 – 249.

[42] It was currently reported that the US Department of Defence to shut down their e-mail system after a hacking attack. See: http://www.defenselink.mil/transcripts/transcript.aspx?transcriptid=3996.

[43] 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.

[44] 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.

[45] An analysis by "Red Sheriff" in 2002 stated that more than 90% of the users worldwide use Microsoft's operating systems (source: www.tecchannel.de - 20.09.2002).

number of advantages to offenders as they can design their attack to be most effective by concentrating only on one target system. The successful attacks carried out by computer viruses and worms do clearly prove the danger of those attacks for countries that depend on the availability of the information infrastructure.[46]

The dependence of society on information technology on the one hand side and the threats of attacks against this infrastructure should influence the development of strategies to prevent attacks. These could contain the development and promotion of technical means of protection as well as ensuring sufficient laws that enable the law enforcement agencies to effectively fight against cybercrime.

B. Number of Users

Currently more than one billion people worldwide use the Internet[47] and it is likely that this number will increase continuously in the coming years. Due to the international dimension of the network the number of possible offenders is significant. Even if only one percent of the users made use of information technology to commit criminal offences the total number of offenders would be more 10 million. The number of users and Internet websites is related to the question how to identify web pages with illegal content within billions of web pages available in the Internet. This is only one example that shows how difficult it is for investigating authorities to fight cybercrime.

C. Availability of Devices

The requirements with regard to the tools that are necessary to commit computer crimes are rather low. In order to commit a cybercrime three elements are in general necessary:

- Hardware
- Software
- Internet Access

Rather cheap computer hardware is available in most countries in the world and its power is increasing continuously.[48] Even without access to the latest generation of computer hardware offenders are able to commit serious crimes. As a matter of fact the criminals are not limited to latest versions of high priced computers but can make use of used computer technology that is less expensive.

In addition to the hardware committing an offence does in many cases require special software tools. Such tools are not only available for sale but are also offered for free download.[49] One of the examples of such tools is software that automatically scans for open ports.[50] Due to the use of mirroring techniques and peer-to-peer exchange it is nearly impossible to prevent the availability of such devices by technical means.[51]

---

[46] A demonstration for the threat of even short interruptions of Internet and computer services was the harm caused by the computer worm "Sasser". In 2004, the computer worm affected computers running vulnerable versions of Microsoft's operation System Windows. As a result of the spreading of the worm a number of offices had to stop their services. Among them the U.S. airline "Delta Airlines" that had to cancel several trans-Atlantic flights because its computer systems had been swamped by the worm; and the electronic mapping services of the British Coastguard was disabled for a few hours. See Heise News, 04.01.2005 – available at: http://www.heise.de/newsticker/meldung/54746; BBC News, Sasser net worm affects millions, 04.05.2004 – available at: http://news.bbc.co.uk/1/hi/technology/3682537.stm.

[47] According to "Internet World Stats" more than 1.15 billion people were using the Internet by 2007 (the statistics are available at: http://www.internetworldstats.com/stats.htm).

[48] Based on the observation by Gordon Moore 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/.

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

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

[51] In order to prevent availability of such tools some countries criminalize the production and offer of such tools. An example of such a provision can be found in Art. 6 Convention on Cybercrime.

Finally, committing cybercrime requires access to the Internet. It is very likely that within the given opportunities the offender will focus on ways to access the Internet that do not allow the law enforcement agencies to identify him or her or at least make their investigations more difficult. Examples for such means of anonymous access are public Internet terminals and open (wireless) networks.[52]

D. Availability of Information

As pointed out above the Internet contains millions of webpages.[53] One of the key elements for the success of the Internet is the possibility to find relevant information from a wide range of available sources. In this context the success of the Internet is not only influenced by the possibility to publish information but also by the existence of powerful search engines that enable the users to search millions of webpages within seconds. "Googlehacking" or "Googledorks" describe the abuse of search engines to filter through large amounts of search results for information related to computer security issues – e.g. with the intention to search for insecure password protection systems.[54] Apart from that, offenders can use the information made available by services like satellite picture providers to prepare an attack.[55] A training manual that was found during investigations against members of a terrorist group highlighted how useful the Internet can be to gather information about possible targets.[56] It was recently discovered that military units that attacked British troops in Afghanistan used satellite pictures taken from Goole Earth to plan their attacks.[57]

E. International Dimension

Very often data transfer processes affect more than one country.[58] This is a result of the design of the network as well as the Internet protocol that ensures that successful transmissions can be made, even if direct lines are temporarily blocked.[59] In addition, a large number of Internet services (like for example hosting services) are offered by companies that are based abroad.[60]

In those cases where the offender is not based in the same country where the victim is located the

---

[52] With regard to the advantages of wireless networks for the development of an IT infrastructure in developing countries see: The Wireless Internet Opportunity for Developing Countries, 2003 – available at: http://www.firstmilesolutions.com/documents/The_WiFi_Opportunity.pdf.

[53] The Internet Systems Consortium identified nearly 490. Million Domains (not to be mixed with webpages) – See: Internet Domain Survey, July 2007 – available at: http://www.isc.org/index.pl?/ops/ds/reports/2007-07/; The Internet monitoring company Netcraft reported in August 2007 that nearly 130 Million websites – available at: http://news.netcraft.com/archives/2007/08/06/august_2007_web_server_survey.html.

[54] 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.

[55] An example is the "Terrorist Handbook" – a pdf-document that contains detailed information on how to build explosives, rockets and other weapons.

[56] "Using public sources openly and without resorting to illegal means, it is possible to gather at least 80% of all information required about the enemy". The reports about the sources of the quotation varies: The British High Commissioner Paul Boateng mentions in a speech in 2007 that the quote was "contained in the Al Qaeda training manual that was recovered from a safe house in Manchester" (see: Boateng, The role of the media in multicultural and multifaith societies, 2007 – available at: http://www.britishhighcommission.gov.uk/servlet/Front?pagename=OpenMarket/Xcelerate/ShowPage&c=Page&cid=1125560437610&a=KArticle&aid=1171452755624. The US Department of Defence reported that the quote was taken from an Al Qaeda Training Manual recovered in Afghanistan (see: http://www.defenselink.mil/webmasters/policy/rumsfeld_memo_to_DOD_webmasters.html). Regarding the availability of sensitive information on websites see: *Knezo*, "Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information, 2006, page 24 – available at: http://digital.library.unt.edu/govdocs/crs/permalink/meta-crs-8704:1.

[57] See http://www.telegraph.co.uk, news from 13 January 2007.

[58] Regarding the extent of transnational attacks in the most damaging cyber attacks see: *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 7 – available at: http://media.hoover.org/documents/0817999825_1.pdf.

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

[60] See *Huebner/Bem/Bem*, Computer Forensics – Past, Present And Future, No.6 – available at: http://www.scm.uws.edu.au/compsci/computerforensics/Publications/Computer_Forensics_Past_Present_Future.pdf; Regarding the possibilities of network storage services see: *Clark*, Storage Virtualisation Technologies for Simplyfing Data Storage and Management.

investigation requires the co-operation of law enforcement agencies in all affected countries.[61] Transnational investigations without the consent of the competent authorities in the countries involved are difficult with regard to the principle of national sovereignty. This principle does in general not allow one country to carry out investigations within the territory of another country without a permission of the local authorities.[62] Therefore the investigations need to be carried out with the support of the authorities of all countries involved. With regard to the fact that in most cases there is only a very short time gap available, in which successful investigations can take place, the application of the classic mutual legal assistance regimes turns out to add to difficulties in Cybercrime investigations as mutual legal assistance in general requires time consuming formal procedures. There are different legislative approach to speed up the investigation. One example is the G8 24/7 Network another one the provisions related to international co-operation in the Council of Europe Convention on Cybercrime.

F. Independence of Place of Action and the Presence at the Crime Site

Committing a cybercrime does in general not require the presence of the perpetrator at the place where the victim is based. This independence of place of action and the location of the victim can add difficulties in regard to cybercrime investigations. Offenders can try to avoid criminal proceedings by acting from countries with weak cybercrime legislation.[63] An effective fight against cybercrime does therefore require the prevention of "safe haven" that would enable the offenders to hide their activities.[64] An example of difficulties resulting from safe havens was the "Love Bug" computer worm that was first discovered in 2000.[65] The computer worm infected millions of computer systems worldwide.[66] Intensive investigations led to a suspect in the Philippines. Due to the fact that the development and spreading of malicious software was at that time not sufficiently criminalized in the Philippines, the local investigation was seriously hindered.[67]

G. Resources

One of the main challenges for law enforcement agencies is the fact that a number of organized crime groups have access to a significant number of computer systems that they can use to carry out automated attacks.[68] An example of the use of a large number of computer systems to carry out an attack was the successful computer attack against government websites in Estonia.[69] Analysis of the attacks point out, that

---

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

[62] National sovereignity is a fundamental principle in International Law. See Roth, State Sovereignity, International Legality, and Moral Disagreement, 2005, page 1 – available at: http://www.law.uga.edu/intl/roth.pdf.

[63] An example are offences related to phishing. Although most sites are stored in the US (32%), China (13%), Russia (7%) and the Republic of Korea (6%) are following. Apart from the US none of them has yet signed and ratified Cybercrime specific international agreements that would enable and oblige them to effectively participate in international investigations.

[64] The issue was addressed by a number of international organizations. The UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies". The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies".

[65] For more information see http://en.wikipedia.org/wiki/ILOVEYOU; regarding the effect of the worm on Critical Infrastructure Protection see: *Brock*, "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000 – available at: http://www.gao.gov/archive/2000/ai00181t.pdf.

[66] BBC News, Police closes 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: http://radsoft.net/news/roundups/luv/20000504,00.html.

[67] See for example: CNN, Love Bug virus raines spectre of cyberterrorism, 08.05.2000, http://edition.cnn.com/2000/LAW/05/08/love.bug/index.html; *Chawki*, A Critical Look at the Regulation of Cybercrime, http://www.crime-research.org/articles/Critical/2; *Sofaer/Goodman*, Cyber Crime and Security – The Transnational Dimension - in *Sofaer/Goodman*, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 10 – available at: http://media.hoover.org/documents/0817999825_1.pdf;

[68] See "Emerging Cybersecurity Issues Threaten Federal Information Systems", GAO, 2005 – available at: http://www.gao.gov/new.items/d05231.pdf.

[69] Regarding the attacks see: Lewis, Cyber Attacks Explained, 2007 – available at: http://www.csis.org/media/csis/pubs/070615_cyber_attacks.pdf; A cyber-riot, The Economist,10.05.2007 – available at: http://www.economist.com/world/europe/PrinterFriendly.cfm?story_id=9163598; Digital Fears Emerge After Data Siege in Estonia, The New York Times, 29.05.2007 – available at: http://www.nytimes.com/2007/05/29/technology/29estonia.html?ei=5070&en=2e77eb21a1ab42ac&ex=1188360000&pagewanted=print.

those attacks could have been committed by thousands of computers that were part of a so called "botnet".[70] Botnets is a term characterizing a group of compromised computers running programmes that are under control of someone.[71] In general the computer that became part of the botnet were previously infected with malicious software that installed a tools that enables the perpetrator to take over the control. Those botnets can for example be used to carry out a denial of service attack[72] or operate file-sharing server.[73]

H. Means of Anonymous Communication

The Internet offers various possibilities for an offender to hide his identity. Using public Internet terminals[74] or an anonymous remailer[75] are just two possibilities to make an identification of an offender difficult or even impossible. Another well-known way to hide identity is to use fake e-mail addresses.[76] Many e-mail services can be used without the need to go through a formal registration process where the entered data are checked. If law enforcement agencies are trying to identify an offender that is using such e-mail address they are at least not able to solely base their investigation on the subscriber information.

III. THE PHENOMENON OF CYBERCRIME AND THE LEGAL RESPONSE

The following chapter will provide an overview about some of the most serious phenomena of cybercrime and the legal response provided by the Convention on Cybercrime. Currently the Council of Europe Convention on Cybercrime[77] is, apart from the UN Resolution 55/63,[78] the only complex international legislative framework in the fight against Cybercrime. Forty five countries signed[79] and 23 countries ratified[80] the Convention on Cybercrime, as of July 2008. With regard to the fact that is was initiated by the Council of Europe, it is important to point out that the Convention is not limited to the Members of the Council of Europe.[81] The Convention on Cybercrime was from the beginning of its drafting designed as an international Convention. Apart from the involvement of the non-members Canada, South-Africa, Japan and the United States, who participated as observers, further non-member states have recently been

---

[70] See: *Toth*, Estonia under cyber attack, http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[71] See: *Ianelli/Hackworth*, Botnets as a Vehicle for Online Crime, 2005, page 3 – available at: http://www.cert.org/archive/pdf/Botnets.pdf;

[72] Regarding the use of botnets in the attacks against computer systems in Estonia see: See: *Toth*, Estonia under cyber attack, http://www.cert.hu/dmdocuments/Estonia_attack2.pdf.

[73] If the offender uses such botnets it is difficult to trace back and identify them as the first traces do only lead to the member of the botnets.

[74] Regarding legislative approaches to require an identification prior to the use of public terminals see Art. 7 of the Italian Decree-Law No. 144.

[75] See: *Claessens/Preneel/Vandewalle*, Solutions for Anonymous Communication on the Internet, 1999.

[76] Regarding the possibilities of tracing an offender by using the e-mail header see: Al-Zarouni, Tracing E-mail Headers, 2004 – available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Al-Zarouni.pdf.

[77] Convention on Cybercrime, European Treaty Series - No. 18. The full text of the Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications are available at: www.coe.int.

[78] A/RES/55/63. The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf (April 2006)

[79] Albania, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Moldova, Montenegro Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Ukraine, United Kingdom, Canada, Japan, South Africa, United States.

[80] Albania, Armenia, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Italy, Latvia, Lithuania, Netherlands, Norway, Romania, Slovakia, Slovenia, The Former Yugoslav Republic of Macedonia, Ukraine, United States.

[81] *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.

(2) In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

invited to accede to the Convention.[82] The Convention contains regulations that, due to the singular status of the Convention, reflect international standards. The importance of the Convention and its relevance as a potential global model law, setting standards for cybercrime legislation cannot be measured solely by the number of signatures or ratifications. A significant number of countries have already made use of the Convention to update their national criminal law in accordance with international standards without formally acceding to the Convention. Examples are Argentina,[83] Pakistan,[84] Philippines,[85] Egypt,[86] Botswana[87] and Nigeria,[88] who have already drafted parts of their legislation in accordance with the Convention.

A. Illegal Access ("Hacking")

1. Phenomenon

Ever since computer networks were developed, their ability to remotely access data on another computer systems has been abused for criminal purposes. The term "hacking" is used to describe the act of unlawfully accessing to a computer system.[89] Due to the fact that many famous computer systems, such as the those of NASA, the Pentagon, Google and the Estonian and German Government, were successfully attacked, hacking has become one of the most well known computer offences.[90] It is one of the oldest computer offences.[91] The first acts of illegal access to a computer system were discovered shortly after the introduction of network technology.[92] But in addition to its long history, the offence has a great relevance in recent times. Entering a computer system without right is very often the first act of combined acts such as phishing[93] and identity theft.[94] The fact, that researches recorded more than 250 million hacking incidents worldwide during the month of August 2007 underlines the relevance of the offence.[95]

Within the scope of recognized offences, the perpetrators' motivations have been wide-ranging.[96] They

[82] Costa Rica, Mexico and the Philippines.

[83] 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).

[84] Draft Electronic Crime Act 2006

[85] Draft Act Defining Cybercrime, providing for Prevention, Suppression and Imposition of Penalties therefor and for other Purposes, House Bill No. 3777.

[86] Draft Law of Regulating the protection of Electronic Data and Information And Combating Crimes of Information, 2006.

[87] Draft Cybercrime and Computer related Crimes Bill 2007, Bill No. 17 of 2007.

[88] Draft Computer Security and Critical Information Infrastructure Protection Bill 2005.

[89] 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.

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

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

[92] With regard to the fact that most criminal law systems did not have such offences the acts could in most countries not be prosecuted until the criminal law was amended.

[93] The term "phishing" describes attempts to fraudulently acquire sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication. See the information offered by anti-phishing working group – available at: www.antiphishing.org; *Jakobsson*, The Human Factor in Phishing – available at: http://www.informatics.indiana.edu/markus/papers/aci.pdf; *Gercke*, CR 2005, 606; The term "phishing" describes an act that is carried out to make the victim disclose personal/secret information. The term "phishing" originally described the use of emails 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*, CR, 2005, 606; *Ollmann*, The Phishing Guide Understanding & Preventing Phishing Attacks – available at: http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf. For more information on the phenomenon of phishing see below: Chapter 2.8.d.

[94] The term identity theft describes the criminal act of fraudulently obtaining and using another person's identity. For more information see: *Gercke*, Internet-related Identity Theft, 2007 – available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_cooperation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf;

[95] 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.

[96] They are ranging from the simple proof that technical protection measures can be circumvented, to the intention of obtaining data stored on the victimized computer.

range from political activism to purely fraudulent intentions. For the perpetrator, access to stored data via a network offers the advantage that security measures at the physical location of the "target" computer, that guard the system against physical access, do not need to be circumvented. In addition, perpetrators do not even have to be present at the crime scene.

2. Legal Response

Taking into account the above mentioned relevance of the offence it might surprise that not all countries criminalize illegal access to a computer system. One example for a country that did for a long time not criminalize illegal access to a computer system is Germany. Until 2007, such acts were intentionally not covered by the German Penal Code.[97] A prosecution was therefore only possible if the offender committed further acts such as the alteration of data.

Analysing the various national approaches to criminalizing illegal access shows a great degree of inconsistence. Some countries, such as Romania, criminalize the mere illegal access to a computer system,[98] while others limit the criminalization by requiring a circumvention of security measures, or harmful intentions, or where data was obtained, modified or damaged during the act.[99] Others do not criminalize mere access, but only subsequent offences.[100]

The Convention on Cybercrime includes a provision on illegal access that protects the integrity of the computer systems by criminalizing unauthorized access to a computer system. The subject of protection is the integrity of computer systems.[101]

(i) Article 2 – Illegal access

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. 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.

The provision does not criminalize a specific method of gaining access to a computer system. To ensure that not every development of new technology requires an amendment of the legislation the provision was drafted by used terms that are neutral with regard to the technology used. The provision requires that the offender acts intentionally[102] and "without right".[103]

Within the implementation of the provision the member states have various possibilities to restrict the application of the provision. They can, for example, require that security measures are circumvented or that the offender acted with a special intent to obtain computer data.

---

[97] See *Gercke*, Comparing the Convention and the current legislation in Germany, MMR 2004, 729.

[98] See for example: Art. 42 Romanian Law No. 161/2003. A country profile that lists the Cybercrime related provisions in the Romanian legislation is available on the Council of Europe website.

[99] Opponents to the criminalization of mere illegal access refer to situations where no dangers were created by mere intrusion, or where the acts of "hacking" led to the detection of loopholes and weaknesses in the security of targeted computer systems. This approach can not only be found in national legislation but was also recommended by the Council of Europe Recommendation N° (89) 9.

[100] An example for this is the German Criminal Code, which criminalized only the act of obtaining data (Section 202a). The provision has recently been changed. The excerpt below was in power until 2007.

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.

[101] Explanatory Report, No. 22.

[102] Explanatory Report to the Council of Europe Convention on Cybercrime, No. 39.

[103] The element "without right" is a common component in the substantive criminal law provisions of the Convention on Cybercrime.

B. Illegal Interception

1. Phenomenon

During transmission processes in a communication network data transfer processes can be intercepted. One example for such interception is the recording of communication in a wireless network. If for example an offender succeeds in intercepting the communication between a computer system and a wireless access point he can intercept all non-encrypted communication such as e-mails sent or received or websites opened. While taking into account the increasing popularity of wireless access and the wireless interconnection of communication devices (e.g. linking mobile communication devices via Bluetooth) it is important to keep an eye on the related vulnerability of the technology with regard to illegal interception.[104]

2. Legal Response

The Convention on Cybercrime includes a provision that protects the integrity of non-public transmission by criminalizing their unauthorized interception.[105] By criminalizing the illegal interception the Convention aims to equate the protection of electronic transfers with the protection of voice phone conversations against illegal tapping.[106]

(i) Article 3 – Illegal interception

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 interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

The provision criminalizes the interception of non-public transmissions. It is neither applicable with regard to public transmissions nor with regard to acts of obtaining information transferred by non-technical means.[107] Based on the definition provided in the Explanatory Report to the Convention on Cybercrime a transmission is "non-public" if the nature of the transmission process is confidential.[108] It is therefore necessary to analyse the status of transmission processes. In general, individual communication (such as sending out an e-mail or downloading information from a website) can be considered non-public. Similar to the provision mentioned above, the acts must be committed intentionally and without right.

C. Data Interference

1. Phenomenon

With regard to the fact that today more and more information is stored in a digital format, the manipulation or destruction of such information can result in great damages. Unlike corporal objects, where the ability to destroy the object in general requires physical access, computer data can in some cases be destroyed without physical access to the storage devices. One example is the use of malicious software such as computer viruses. Computer viruses are software tools that are - without permission - installed on the victim's computer in order to carry out operations such as the deletion of data.[109] Like illegal access, data interference can be considered a traditional computer crime. The first computer viruses appeared in

---

[104] *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime" in Cybercrime & Security, IIA-2, page 6 et seqq.

[105] Like Art. 2, Art. 3 enables the signatory states to adjust the extent of the criminalization within the implementation process by requiring additional elements like "dishonest intent" or the relation to a computer system that is connected to another computer system.

[106] Explanatory Report No. 60.

[107] Within this context only interceptions made by technical means are covered by the provision - Article 3 does not cover acts of "social engineering".

[108] Explanatory Report, No. 54.

[109] See *Spafford*, "The Internet Worm Program: An Analysis", page 3; *Cohen*, "Computer Viruses - Theory and Experiments" – available at: http://all.net/books/virus/index.html. *Cohen*, "Computer Viruses"; *Adleman*, "An Abstract Theory of Computer Viruses". Regarding the economic impact of computer viruses, see *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12; Symantec "Internet Security Threat Report", Trends for July-December 2006 – available at: http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf

the 1970s.[110] Since then, not only the number of computer viruses but also the damage they cause has risen significantly.[111] The emerging use of networks enable the viruses to spread much quicker than in those times, where the exchange of disks was the main way of distribution. One example is the "Love Bug" computer worm that was developed by a suspect in the Philippines in 2000[112] and infected millions of computers worldwide.[113] The increasing speed of distribution influenced the damage caused by virus attacks. In 2000 the financial loss caused by malicious software was estimated to an amount of up to 17 billion US$.[114]

2. Legal Response

In Article 4, the Convention on Cybercrime includes a provision that protects the integrity of data against unauthorized interference.[115] The aim of the provision is to fill the existing gap in some national penal laws and to provide computer data and computer programmes with a protection similar to those enjoyed by corporeal objects against the intentional infliction of damage.[116]

(i) 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.

The provision not only criminalizes the damage and deletion of computer data, e.g. by computer virus.[117] In addition to traditional manipulations the drafters of the Convention decided to include acts that can lead to similar damages. One example is the alteration of computer data. If a computer virus randomly changes the content of a document the damage can be comparable to a deletion of the file. Similar to the provisions mentioned above, the acts must be committed intentionally and without right.

D. System Interference

1. Phenomenon

Information technology has become an important element of business communication and operation. As pointed out previously,[118] the integration of computer technology in the everyday life reached a level that the information societies are depending on the availability of those services. The interruption of important

---

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

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

[112] For more information, see http://en.wikipedia.org/wiki/ILOVEYOU; regarding the effect of the worm on Critical Information Infrastructure Protection, see: *Brock*, "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities, 2000, available at: http://www.gao.gov/archive/2000/ai00181t.pdf.

[113] 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.

[114] *Cashell/Jackson/Jickling/Webel*, "The Economic Impact of Cyber-Attacks", page 12 – available at: http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf. The fact that the number of people using the Internet has increased since then, but that the estimated losses have decreased, shows that the number of users of networks is only one aspect that influences development.

[115] Article 4 is offers the possibility of restricting criminalization by limiting it to cases where the actions result in serious harm.

[116] Explanatory Report, No. 60.

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

[118] See above: Chapter 1.

services can have a negative impact on the development of the society.[119] If, for example, servers that are responsible for providing communication services are not available, the users have to switch to alternative means of communication. The existence of alternative means of communication is very likely an essential part of a Cyber-Security strategy of most global businesses but due to the cost of keeping redundant systems available it is not likely that they are available to the majority of Internet users.[120]

Affecting the availability of services can take place in various ways. The impact of the damage to the undersea cable in 2008, which was very likely caused by anchoring ships, led to a dramatic decrease of the transmission speed in the Asian Pacific region and shows the potential of accidents.[121] But in addition to accidental interruption there are various ways in which offenders can influence the availability of Internet services. One possibility is the physical termination of critical infrastructure – e.g. the physical damage of an Internet server. A way to hinder a computer system from operating without being present at the physical location of the server is the installation of a computer virus that deletes important files on the computer system.[122] But a successful attack with a computer virus requires the circumvention of protection measures. With regard to fact that depending on the configuration of the protection system can have unique difficulties, a third possibility of interfering with the functioning of a computer system has become very popular in recent times. A number of famous web pages[123] became victims of so-called "Denial-of-Service (DOS) attacks".[124] Within such attacks the offenders are targeting a computer system with more requests than the computer system can handle.[125] Even powerful systems can be affected by these attacks.

---

[119] This is especially relevant with regard to the trust of the users. If due to frequent unavailability of critical services the users loose the trust in the reliability of the provider this can seriously influence it's operations. Regarding the importance of trust in e-commerce see: *Ratnasingham*, The importance of trust in electronic communication, Internet Research, 1998, Vol. 8, Issue 4, page 313 et. Seqq; *Meech/Marsh*, Social Factors in E-Commerce Personalization – available at: http://iit-iti.nrc-cnrc.gc.ca/iit-publications-iti/docs/NRC-43664.pdf; *Shim/Van Slyke/Jiang/Johnson*, Does Trust reduce concerns for information privacy in e-commerce? – available at: http://sais.aisnet.org/2004/.%5CShim,%20VanSlyke,%20Jiang%20&%20Johnson.pdf.

[120] As a consequence, the fact that a business provides a redundant system for communication does not necessary mean that the ability to communicate with it's customers is not affected if the main communication system fails as the users might not have the ability to switch means of communication.

[121] Regarding the underwater cable damage see for example: US Department of Homeland Security, Daily Open Source Infrastructure Report, 4 February 2008 – available at: http://www.globalsecurity.org/security/library/news/2008/02/dhs_daily_report_2008-02-04.pdf; Hamblen, A third underwater cable is cut in Middle East, Computerworld, 1 February 2008 – available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9060658; New cable cut compounds net woes, BBC News, 4 February 2008 – available at: http://news.bbc.co.uk/2/hi/technology/7222536.stm.

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

[123] *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;

[124] In 2004 the web-services of the German Airline Lufthansa was affected by such a DOS-attack. As a result the use of the online booking-service was not or only with delay available for the period of 2 hours.

[125] A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, "Analysis of a Denial of Service Attack on TCP"; *Houle/Weaver*, "Trends in Denial of Service Attack Technology", 2001, available at: http://www.cert.org/archive/pdf/DoS_trends.pdf.In 2000 a number of well known US e-commerce businesses were targeted by denial of service attacks. A full list of the attacks business is provided by *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", page 4, available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.For more information see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000 – available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20 – available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, "Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and

2. Legal Response

In order protect the interest of operators and users to have appropriate access to telecommunication technology the Convention on Cybercrime includes in Article 5 a provision that criminalizes the intentional hindering of the lawful use of computer systems.

(i) Article 5 – System interference

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 serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

The provision does not criminalize specific acts that lead to system interference but covers any activity that interferes with the proper functioning of the computer system.[126] This covers physical termination of a server as well as computer viruses or a DoS attack. The fact that the provision limits the criminalization to serious attacks enables the signatory states to the Convention to limit the criminalization to attacks against important services or attacks that caused significant damage.[127] The act must be committed intentionally and without right.

E. Misuse of Devices

1. Phenomenon

A serious issue concerning cybercrime is the availability of software and hardware tools designed to commit crimes. Most of these devices are available on a large scale, the majority distributed for free. They are easy to operate and can therefore even be run by users without any specific technical knowledge. Such software can be used for the interception of wireless communication or the identification of open wireless networks ("Wardriving[128]"), the decryption of encrypted files or to run Denial of Service (DOS)[129] attacks. With regard to the fact, that the commission of these offences often requires the possession of tools, there is a strong incentive to acquire them for criminal purposes, which could lead to the creation a kind of black market for their production and distribution. Apart from the proliferation of "hacking devices", the exchange of passwords that enable the unauthorized user to access a computer system is taking place on a large scale.

2. Legal Response

Facing this development, the drafters of the Convention decided to establish an independent offence criminalizing specific illegal acts regarding certain devices or access to data that can be misused for the purposes of committing offences against the confidentiality, integrity and availability of computer systems or data.[130]

(i) Article 6 – Misuse of Devices

(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 and without right:

Implications for the Department of Homeland Security", Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3 – available at: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[126] Explanatory Report, No. 66.

[127] Although the connotation of "serious" does limit the applicability, it is likely that even serious delays of operations resulting from attacks against a computer system can be covered by the provision.

[128] Wardriving is a term used to characterize the search for wireless networks (WLAN / Wi-Fi) by moving vehicles. As long as the search for wireless networks does not go along with the misuse of the networks the legality of this action is in most countries not clearly defined. Regarding the situation in Germany see Baer, Wardriver, MMR 2005, 434.

[129] A Denial-of-Service (DoS) attacks aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors for Distributed Denial-of-Service Attacks", available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html;

[130] Due to the controversial discussion on the need for criminalization of the possession of the devices, the Convention is – in addition to Paragraph 1 b) Sentence 2 - offering the option of a complex reservation in Article 6 Paragraph 3. If a Party makes use of this reservation it can exclude the criminalization for the possession of tools and a number of illegal actions under Paragraph 1) a) – e.g. the production of such devices.

(a) the production, sale, procurement for use, import, distribution or otherwise making available of:

(i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
(ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,
with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

(b) the possession of an item referred to in paragraphs a) i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

(2) This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.

(3) Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

The threat of these devices makes it difficult to focus the criminalization on the use of these tools to commit crimes only. Most of the national criminal law systems do, in addition to the "attempt of an offence", have some provision criminalizing acts of preparation of crimes. In general this criminalization – which goes along with an extensive forward displacement of criminal liability – is limited to the most serious crimes. Especially in EU legislation, there are tendencies to extend the criminalization to preparatory acts to less grave offences.[131]

The connection factor of criminalization as established by Paragraph 1 (a) are on the one hand devices[132] designed to commit cybercrimes and on the other hand passwords that enable access to a computer system. With regard to these items, the Convention criminalizes a wide range of actions. In addition to production, it sanctions the sale, procurement for use, import, distribution or otherwise making available of the devices and passwords. A similar approach (but limited to devices designed to circumvent technical measures) can be found in EU legislation regarding the harmonization of copyrights.[133]

F. Computer-Related Forgery

1. Phenomenon

Due to the shift from classic tangible documents to electronic documents the forgery of computer-related data is playing an increasing role. The offence has especially become very popular with regard to "phishing"

---

[131] An example is the EU Framwork Decision ABl. EG Nr. L 149, 2.6.2001.

[132] With it's 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 indicate a restriction of devices to software. Although the Explanatory Report is not certain in this matter it is likely that not only software devices are covered by the provision but hardware tools as well.

[133] 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.

attacks.[134] The term "phishing" is used to describe a type of crime that is characterized by attempts to fraudulently acquire sensitive information, such as passwords, by masquerading as a trustworthy person or business (e.g. financial institution) in an apparently official electronic communication.[135] Most of these phishing attempts are operated via e-mail. The person receiving such e-mail is for example ordered to verify his online bank account ("Click here to verify your account") and by entering his or her account number and password on a webpage that was set up by the offenders, the offenders get access to the data.

2. Legal Response

The criminalization of the forgery of tangible items has a long legal tradition in most countries.[136] The Convention aims to create a parallel offence to the forgery of tangible documents in order to fill gaps in criminal law related to traditional forgery, which require visual readability of statements or declarations embodied in a document and therefore do not apply to electronically stored data.[137]

(i) Article 7 – Computer-Related forgery

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 and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

The target of a computer-related forgery is only data – not depending on whether they are directly readable and intelligible. To draw the line on the forgery of tangible documents Article 7 requires – at least with regard to the mental element - that the data is the equivalent of a public or private document. This includes the need for legal relevance. The forgery of data that cannot be used for legal purposes is therefore not covered by the provision.

---

[134] 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.

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

[136] See for example 18 U.S.C. § 495:

Whoever falsely makes, alters, forges, or counterfeits any deed, power of attorney, order, certificate, receipt, contract, or other writing, for the purpose of obtaining or receiving, or of enabling any other person, either directly or indirectly, to obtain or receive from the United States or any officers or agents thereof, any sum of money; or Whoever utters or publishes as true any such false, forged, altered, or counterfeited writing, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited; or

Whoever transmits to, or presents at any office or officer of the United States, any such writing in support of, or in relation to, any account or claim, with intent to defraud the United States, knowing the same to be false, altered, forged, or counterfeited – Shall be fined under this title or imprisoned not more than ten years, or both.

A similar approach can be found in 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.

[137] Explanatory Report, No. 81.

G. Computer-Related Fraud

1. Phenomenon

Fraud remains one of the most popular crimes in cyberspace. Especially the success of online shopping and Internet auctions increased the opportunities of offenders. The most popular crimes are credit card fraud and auction fraud.[138] Apart from that, the development of assets administered in computer systems (electronic funds, deposit money, e-gold) has become the target of manipulations. To avoid these criminal acts, especially with regard to Internet auctions, a number of confidence-building measures have been taken on the technical side.[139] But the missing personal contact between the seller and customer limits the possibilities of self-protection.

As fraud is a common problem outside the Internet as well, most national laws contain provisions criminalizing such offences. The application of those provisions to Internet-related cases can be difficult if the traditional national criminal law provisions relate to a falsity of a person.[140] In many cases of fraud committed on the Internet the offender is manipulating a computer system. If the traditional provisions that criminalize fraud do not apply to computer-systems an update of the national law is necessary.

2. Legal Response

The Convention is aiming to criminalize any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property by providing an Article regarding computer-related fraud.[141]

(i) Article 8 – Computer-Related fraud

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 and without right, the causing of a loss of property to another person by:

a. any input, alteration, deletion or suppression of computer data;
b. any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 8 combines the most relevant acts with regard to computer-related fraud (input, alteration, deletion and suppression) with the general act "interference with the functioning of a computer system" in order to open the provision for further developments.[142]

In most national criminal law systems the fraud must lead to an economic loss. In addition to a general intent with regard to the elements of crime (especially the manipulation) Art. 8 therefore requires a special fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. As an example of acts excluded from criminal liability because of a missing special intent the Explanatory Report mentions commercial practices with respect to market competition that may cause an economic detriment to a person and a benefit to another, but are not carried out with fraudulent or dishonest intent.[143]

---

[138] "Law Enforcement Efforts to combat Internet Auction Fraud", Federal Trade Commission, 2000, page 1, available at: http://www.ftc.gov/bcp/reports/int-auction.pdf; *Beales*, Efforts to Fight Fraud on the Internet, Statement before the Senate Special Committee on aging, 2004, page 7 – available at: http://www.ftc.gov/os/2004/03/bealsfraudtest.pdf.

[139] An example for this is the service offered by PAYPAL: PAYPAL is an internet business that enables the user to transfer money, avoiding traditional paper methods such as money orders. It also performs payment processing for auction sites.

[140] An example of this is Section 263 of the German Penal Code that requires the falsity of a person (mistake). The provision does therefore not 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.

[141] Explanatory Report, No. 86.

[142] As a result not only data related offences but also hardware manipulations are covered by the provision.

[143] 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, No. 90.

H. Child Pornography

1. Phenomenon

During the last years the Internet has become the primary instrument for trading child pornography.[144] There are two main reasons for this development:

- The Internet offers unique possibilities with regard to the dissemination of content. By making a file available in a file-sharing system it can be downloaded by millions of users worldwide. This increases the number of potential consumers compared to traditional ways of distribution.

- A second reason for the success of web pages with pornographic material is the fact that users are considering themselves to be less "visible" while gaining access to the material online compared to accessing a regular shop. This is an advantage for investigation as most users do not even know about the traces they leave while surfing in the Internet.[145]

2. Legal Response

In order to improve the protection of children against sexual exploitation by modernizing criminal law provisions, the Convention provides an Article dealing with child pornography.

(i) Article 9 – Offences related to child pornography

(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 and without right, the following conduct:

a) producing child pornography for the purpose of its distribution through a computer system;
b) offering or making available child pornography through a computer system;
c) distributing or transmitting child pornography through a computer system;
d) procuring child pornography through a computer system for oneself or for another person;
e) possessing child pornography in a computer system or on a computer-data storage medium.

(2) For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct;
b) a person appearing to be a minor engaged in sexually explicit conduct;
c) realistic images representing a minor engaged in sexually explicit conduct.

(3) For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

(4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

It is important to point out two controversial discussed elements of the offence established by Article 9: The criminalization of the possession of child pornography and the integration of fictional images.

Within its approach to improve the protection of minors against sexual exploitation the Council of Europe introduced a new Convention in 2007.[146] On the first day the Convention was opened for signature 23 states signed the Convention.[147] One of the key aims of the Convention is the harmonization of criminal

---

[144] *Krone*, A Typology of Online Child Pornography Offending, Trends & Issues in Crime and Criminal Justice, No. 279.

[145] Regarding the possibilities to trace back offenders of computer-related crimes see: *Lipson*, Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues.

[146] Council of Europe - Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No. 201).

[147] 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. Denmark, Iceland, Italy, Ukraine and the United Kingdom followed (July 2008).

law provisions that aim to protect children from sexual exploitation.[148] To achieve this aim the Convention contains a set of criminal law provisions. Apart from the criminalization of the sexual abuse of children (Art. 18) the Convention contains provisions dealing with the exchange of child pornography (Art. 20) and the solicitation of children for sexual purposes (Art. 23).

(ii) Article 20 – Offences concerning child pornography

(1) Each Party shall take the necessary legislative or other measures to ensure that the following intentional conduct, when committed without right, is criminalized:

a) producing child pornography;
b) offering or making available child pornography;
c) distributing or transmitting child pornography;
d) procuring child pornography for oneself or for another person;
e) possessing child pornography;
f) knowingly obtaining access, through information and communication technologies, to child pornography.

(2) For the purpose of the present article, the term "child pornography" shall mean any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes.

(3) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.a and e to the production and possession of pornographic material: – consisting exclusively of simulated representations or realistic images of a non-existent child; – involving children who have reached the age set in application of Article 18, paragraph 2, where these images are produced and possessed by them with their consent and solely for their own private use.

(4) Each Party may reserve the right not to apply, in whole or in part, paragraph 1.f.

(iii) Article 23 – Solicitation of children for sexual purposes

Each Party shall take the necessary legislative or other measures to criminalize the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.

Art. 20 of the Convention on the protection of children is to a large degree comparable to Art. 9 of the Convention on Cybercrime. The first main difference is the fact that the Convention on Cybercrime focuses on the criminalization of acts related to information and communication services ("producing child pornography for the purpose of its distribution through a computer system") while the Convention on the Protection of Children follows a broader approach ("producing child pornography") and even covers acts that are not related to computer networks. In addition Art. 20 (1) f) of the Convention on the Protection of Children criminalizes the act of obtaining access to child pornography.[149] The Convention on Cybercrime does not contain such a provision.

Art. 23 Convention on the protection of children criminalizes the solicitation of children for sexual purposes by means of information and communication technology. The Convention on Cybercrime does not contain such a provision.

I. Copyright Crimes

1. Phenomenon

The switch from analogue to a digital distribution of music and videos led to new forms of copyright

[148] For more details see *Gercke*, ZUM 2008, 550ff.

[149] The provision is especially relevant in those cases where the offender is accessing information in a computer network without downloading it. In those cases the access to the information is – depending on the configuration of the computer system and the services used - not in accordance with a possession of the information.

violations. Millions of copyright protected songs and movies are exchanged in file-sharing systems every day.[150] Some movies even appeared in file-sharing systems before their world premiere in cinema.[151]

The entertainment industry responded by implementing technical measures (DRM) to prevent reproduction,[152] but until now these measures have always been circumvented shortly after their introduction. A number of software tools are available that enable the user to copy music CD's and movie DVD's that are protected by DRM-systems. In addition, the Internet offers the possibility to distribute the copies worldwide. As a result, the infringements of intellectual property rights are among the most commonly committed offences on the Internet.

2. Legal Response

The Convention contains a provision that aims to harmonize the various approaches to criminalize copyright violations in the national laws of the signatory states.

Article 10 – Offences related to infringements of copyright and related rights

(1) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

(2) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under 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 and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

(3) A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

One of the main differences between Art. 10 Convention on Cybercrime and most national approaches is the fact that Art. 10 does not explicitly name those acts that are supposed to be criminalized, but refers to a number of international agreements – such as the WIPO Copyright treaty. This led to criticism from those countries that are not members of WIPO.[153]

The criminalization[154] of copyright crimes established by Art. 10 Convention on Cybercrime is limited to serious cases and therefore excludes minor violations of copyrights.[155] In addition the Convention does only cover

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

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

[152] The technology that is used is called Digital Rights Management – DRM. The term Digital rights management (DRM) is used to describe several technologies used to enforce pre-defined policies controlling access to software, music, movies, or other digital data. One of the key functions is the copy protection that aims to control or restrict the use and access to digital media content on electronic devices with such technologies installed.

[153] In this context it is important to highlight that the signature of the Convention does not oblige the states to become members of the WIPO. It is sufficient to implement criminalization for those violations mentioned in Art. 10 Convention on Cybercrime.

[154] Paragraph 3 enables the parties to make a reservation and not criminalize copyright violations as long as they provide that other effective remedies are available and the reservation does not derogate from the parties' international obligations.

[155] The Convention is designed to set minimum standards for Internet-related offences. Therefore parties can go beyond the threshold of "commercial scale" in the criminalization of copyright violations.

acts that are committed by the means of a computer system. Copyright violations that do not involve information technology are not covered by the provision. Another major limitation of the criminalization is granted by the requirement of a violation on a commercial scale. A similar restriction is contained in the TRIPS Agreement, which requires criminal sanctions only in the case of "piracy on a commercial scale". As most of the copyright violations in file-sharing systems are not committed on a commercial scale they are not covered by Article 10.

IV. PROCEDURAL INSTRUMENTS CONTAINED IN THE CONVENTION ON CYBERCRIME

As pointed out previously, cybercrime investigations involve a number of unique challenges, such as the high speed of data exchange processes. To be able to react to the challenges, law enforcement agencies need procedural instruments that enable them to take those measures that are necessary to identify the offender and collect the evidence required for criminal proceedings.[156] With regard to the special challenges related to cybercrime investigation the traditional investigation instruments, such as search and seizure, will not be sufficient to carry out successful investigations. The Convention on Cybercrime therefore contains a set of special instruments.

A. Expedited Preservation of Data

1. The Situation

The identification of a cybercrime offender very often requires the analysis of traffic data.[157] In particular, the IP address used by the offender while committing the offence is an important information that can help to trace him or her back. One of the main challenges for investigation is the fact that traffic data that are relevant for the identification are often deleted automatically within a rather short period of time.[158] Some countries have strict laws that prohibit the storage of certain traffic data after the end of a process. One example for such restriction is Art. 6 EU Directive on Privacy and Electronic Communication.[159]

2. The Related Procedural Instrument

Art. 16 Convention on Cybercrime enables the law enforcement agencies to order the preservation of traffic as well as content data ("quick freeze").

Article 16 – Expedited preservation of stored computer data

(1) Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

(2) Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified

---

[156] Regarding user-based approaches in the fight against Cybercrime see: *Goerling*, The Myth Of User Education, 2006 - www.parasite-economy.com/texts/StefanGorlingVB2006.pdf. See as well the comment made by *Jean-Pieree Chevenement*, French Minister of Interior, at the G8 Conference in Paris in 2000: "More broadly, we have to educate users. They must all understand what they can and can't do on the Internet and be warned of the potential dangers. As use of the Internet grows, we'll naturally have to step up our efforts in this respect."

[157] "Determining the source or destination of these past communications can assist in identifying the identity of the perpetrators. In order to trace these communications so as to determine their source or destination, traffic data regarding these past communications is required", See: Explanatory Report to the Council of Europe Convention on Cybercrime No. 155.; Regarding the identification of suspects by IP-based investigations see: *Gercke*, Preservation of User Data, DUD 2002, 577 et. seqq.

[158] The reason for this automated deletion process is the fact that after the end of a process (e.g. sending out an e-mail, accessing the Internet or downloading a movie) those traffic data that have been generated during the process and that ensure that the process could be carried out are not anymore needed and the storage of the data would increase the cost of operating the service. The cost issue was especially raised within the discussion about data retention legislation in the EU. See for example: E-communications service providers remain seriously concerned with the agreement reached by EU Justice Ministers to store records of every e-mail, phone call, fax and text message, Euroispa press release, 2005 – available at: http://www.ispai.ie/EUROISPADR.pdf; See as well: ABA International Guide to Combating Cybercrime, page 59.

[159] 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.

stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

This instrument should enable the law enforcement agencies to react immediately after becoming aware of an offence and avoid the risk of a deletion as a result of long lasting procedures.[160] After receiving such order the providers are obliged to preserve those data that were processed during the operation of the service.[161] Art. 16 does not include an obligation of an Internet Service Provider to transfer the relevant data to the authorities. The transfer obligation is regulated in Art. 17 and 18 Convention on Cybercrime.

In this context it is important to highlight that Art. 16 does not contain a data retention obligation. A data retention obligation forces the provider of Internet services to save all traffic data for a certain period of time.[162] This would enable the authorized agencies to gain access to data that is necessary to identify an offender even month after the perpetration.[163] A data retention obligation was recently adopted by the EU Parliament[164] and is currently discussed in the US.[165]

B. Production Order

1. The Situation

As mentioned above Art. 16 does only oblige the provider to save those data that were processed by the provider and not deleted at the time the provider receives the order.[166] The provision does not oblige the provider to transfer the relevant data to the authorities.

2. The Related Procedural Instrument

The transfer obligation is regulated in Art. 18 Convention on Cybercrime.

Article 18 – Production order

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its

[160] 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.

[161] '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.

[162] Regarding The Data Retention Directive in the EU 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. seqq.

[163] See: Preface 11. of the EU 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."

[164] 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.

[165] 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: http://www.govtrack.us/congress/bill.xpd?bill=h110-837. Regarding the current situation in the US see: ABA International Guide to Combating Cybercrime, page 59.

[166] '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.

competent authorities to order:

a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

(2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

(3) For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a) the type of communication service used, the technical provisions taken thereto and the period of service;
b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Art. 18 of the Convention on Cybercrime is not only applicable after a preservation order is issued: the provision is a general instrument that law enforcement agencies can make use of. If the Internet Service Providers are voluntarily transferring the requested data law enforcement agencies are not limited to seizing hardware but can make use of the less intensive production order.

C. Partial Disclosure of Traffic Data

1. The Situation

As pointed out previously, the Convention strictly divides between the obligation to preserve data on request and the obligation to disclose them to the competent authorities.[167]

2. The Related Procedural Instrument

Art. 17 combines the obligation to ensure the preservation of traffic data in cases where a number of service providers were involved with the additional obligation to disclose the necessary information in order to enable the LEAs to identify the path through.

Article 17 – Expedited preservation and partial disclosure of traffic data

(1) Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a) ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

(2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Without such partial disclosure law enforcement agencies would in some cases not be able to trace back the offender and preserve more relevant data when more than one provider was involved in a data exchange process.[168]

[167] *Gercke*, The Convention on Cybercrime, MMR 2004, 802.

[168] "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.

D. Submission of Subscriber Information

1. The Situation

The main aim of most cybercrime investigations is the identification of the suspects involved in committing the offences. Therefore the individualization of the suspect is a major aim of the procedural instruments. Such identification can be achieved with the help of subscriber information. The use of many Internet services, such as the access to the Internet or the rental of server storage require registration. The subscriber information submitted during the registration process can enable the individualization process.

2. The Related Procedural Instrument

In addition to the obligation to submit computer data, Art. 18 CoC enables law enforcement agencies to order the submission of subscriber information.

Article 18 – Production order

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a) a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
b) a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

(2) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

(3) For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a) the type of communication service used, the technical provisions taken thereto and the period of service;
b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

This investigation instrument is of great importance in IP-based investigations. If the law enforcement agencies are able to identify an IP-address that was used by the offender while carrying out the offence they will need to identify the person[169] who used the IP-address at the time of the offence. Based on Art. 18 Subsection 1 b) Convention on Cybercrime a provider is obliged to submit those subscriber information listed in Art. 18 Subsection 3 Convention on Cybercrime.

E. Search

1. The Situation

Search and seizure is one of the most important instruments in cybercrime investigation.[170] Search and seizure of tangible objects is a traditional investigation instrument in most criminal procedural codes.[171] The reason why the drafters of the Convention on Cybercrime nevertheless included a provision dealing with search and seizure is the fact that national laws often do not cover data-related search and seizure

[169] 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.

[170] A detailed overview about the elements of search procedures is provided by the ABA International Guide to Combating Cybercrime, 123 et. seqq. For more information on Computer-related Search and Seizure see: *Winick*, Searches and Seizures of Computers and Computer Data, Harvard Journal of Law & Technology, 1994, Vol. 8, page 75 et seqq.; *Rhoden*, Challenging searches and seizures of computers at home or in the office: From a reasonable expectation of privacy to fruit of the poisonous tree and beyond, American Journal of Criminal Law, 2002, 107 et seqq.

[171] See Explanatory Report to the Convention on Cybercrime, No. 184.

procedures.[172] Based on such provision the investigators would be able to seize an entire server but not seize only the relevant data by copying them.[173]

2. The Related Procedural Instrument

(i) Article 19 – Search and seizure of stored computer data

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a. a computer system or part of it and computer data stored therein; and
b. a computer-data storage medium in which computer data may be stored in its territory.

(2) Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

[...]

Art. 19 sub-paragraph 1 of the Convention on Cybercrime aims to establish an instrument that enables investigators to search computer systems as efficiently as they are able to perform traditional search procedures.[174] Art. 19 sub-paragraph 2 of the Convention on Cybercrime addresses a growing problem within cybercrime related investigations. During the search for information at the physical location of a computer system investigators frequently realize that the suspect did not store the relevant information (e.g. child pornography) on local hard drive but on an external server which he can access via Internet.[175] Using Internet servers to store data is becoming more and more popular.[176] To ensure that investigations can be carried out efficiently it is important to maintain a certain flexibility of investigations. If the investigators discover that the relevant information is stored in another computer system they should be able to extend the search to this system.[177]

F. Seizure

1. The Situation

The examination of computer systems and especially internal and external storage devices is an

[172] "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.

[173] This can cause difficulties in those cases where the relevant information are stored on a server with the data of hundreds of other users that would not be available anymore when law enforcement agencies seize the server.

[174] "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.

[175] The importance of being able to extend the search to connected computer systems was already addressed by the Council of Europe Recommendation No. R (95) 13 of he Committee of Ministers to Member States concerning problems of criminal procedural law connected with information technology that was adopted by the Committee of Ministers on 11.09.1995 at the 543rd meeting of the Ministers Deputies. The text of the Recommendation is available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/1_standard_settings/Rec_1995_13.pdf

[176] One of the advantages of storing the information on Internet servers is the fact that the information can be accessed from any place with Internet connection.

[177] 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 as well: New Jersey Computer Evidence Search and Seizure Manual, 2000, page 12 – available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

important aspect of computer forensics.[178] In general an investigation of the storage devices requires physical access to the hardware.[179]

2. The Related Procedural Instrument

(i) Article 19 – Search and seizure of stored computer data

[…]

(3) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a) seize or similarly secure a computer system or part of it or a computer-data storage medium;
b) make and retain a copy of those computer data;
c) maintain the integrity of the relevant stored computer data;
d) render inaccessible or remove those computer data in the accessed computer system.

(4) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

Art. 19 sub-paragraph 3, Convention on Cybercrime enables the law enforcement agencies to seize computer hardware.[180] In addition to the tradition of seizure of the hardware, the Convention on Cybercrime enables the law enforcement agencies to copy the relevant data instead of seizing the hardware.[181] If the law enforcement agencies decide not to seize the hardware but only to copy the relevant data there are a number of side-measures provided by Art. 19 Convention on Cybercrime to maintain the integrity of the copied data and remove the original data.[182]

Very often the investigators will not be able to identify the exact location of relevant data without the help of the system administrator that is responsible for the server infrastructure.[183] But even if they are able to identify the hard drive protection measures might stop them from searching for the relevant data.

---

[178] *Hannan*, To Revisit: What is Forensic Computing, 2004 – available at: http://scissec.scis.ecu.edu.au/publications/forensics04/Hannan.pdf; *Etter*, The forensic challenges of e-crime, Australasian Centre for Policing Research, No. 3, 2001, page 4 – available at: http://www.acpr.gov.au/pdf/ACPR_CC3.pdf;

[179] Regarding the advantages of remote forensic tools compared with traditional search and seizure procedures see *Gercke*, Secret Online Search, CR 2008, page 245 et. seqq. But there are also disadvantages related to remote investigations. Apart from the fact that direct access enables the law enforcement agencies to examine the physical condition of storage media physical access to a computer system it is the only way to ensure that the files on the suspects computer are not modified during the investigation. Regarding the importance of protecting the integrity of the examined computer system see: *Meyers/Rogers*, Computer Forensics: The Need for Standardization and Certification, page 6 – available at: http://www.utica.edu/academic/institutes/ecii/publications/articles/A0B7F51C-D8F9-A0D0-7F387126198F12F6.pdf.

[180] For guidelines how to carry out the seizure of computer equipment see for example: General Guidelines for Seizing Computers and Digital Evidence, State of Maryland, Maryland State Police, Criminal Enforcement, Command, Computer Crimes Unit, Computer Forensics Laboratory – available at: http://ccu.mdsp.org/Guidelines%20-%20Seizure%20of%20Digital%20Evidence.htm; New Jersey Computer Evidence Search and Seizure Manual, State of New Jersey, Department of Law and Public Safety, Division of Criminal Justice – available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[181] Regarding the classification of the act of copying the data see: *Brenner/Frederiksen*, Computer Searches and Seizure: Some Unresolved Issues in Cybercrime & Security, IB-1, page 58 et seqq.

[182] "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.

[183] "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 recognizes 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.

The drafters of the Convention therefore included an obligation of system administrator and other people, who have knowledge about the location of stored information to assist the law enforcement agencies.

G. Collection of Traffic Data

1. The Situation

Traffic data play an important role in cybercrime investigation.[184] Having access to content data enables the law enforcement agencies to analyse the nature of messages of files exchanged and help to trace the offender. By monitoring the traffic data generated during the use of Internet services, law enforcement agencies are able to identify the IP-address of the server and can then try to determine the physical location of the offender.

2. The Related Procedural Instrument

With Art. 20 the Convention on Cybercrime provides the legal basis for the real time collection of traffic data.

(i) Article 20 – Real-time collection of traffic data

(1) Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and
b) compel a service provider, within its existing technical capability:

i) to collect or record through the application of technical means on the territory of that Party; or
ii) to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

*(4) The powers and pro*cedures referred to in this article shall be subject to Articles 14 and 15.

The provision is neither drafted with preference to a specific technology nor is it intending to set standards that go along with the need for high financial investments for the industry involved.[185]

H. Interception of Content Data

1. The Situation

In some cases the collection of traffic data is not sufficient to collect the evidence that is required to convict the suspect. This is especially relevant in those cases where the law enforcement agencies do already know the communication partners and the services used but have no information about the information exchanged.

---

[184] "In case of an investigation of a criminal offence committed in relation to a computer system, traffic data is needed to trace the source of a communication as a starting point for collecting further evidence or as part of the evidence of the offence. Traffic data might last only ephemerally, which makes it necessary to order its expeditious preservation. Consequently, its rapid disclosure may be necessary to discern the communication's route in order to collect further evidence before it is deleted or to identify a suspect. The ordinary procedure for the collection and disclosure of computer data might therefore be insufficient. Moreover, the collection of this data is regarded in principle to be less intrusive since as such it doesn't reveal the content of the communication which is regarded to be more sensitive." See: Explanatory Report to the Convention on Cybercrime, No. 29. Regarding the importance of traffic data in Cybercrime investigations see as well: ABA International Guide to Combating Cybercrime, page 125; *Gercke*, Preservation of User Data, DUD 2002, 577 et. seqq.

[185] "The article [Art. 20] does not obligate service providers to ensure that they have the technicalcapability 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.

2. The Related Procedural Instrument

Art. 21 enables the law enforcement agencies to record data communication and analyse the content.[186]

(i) Article 21 – Interception of content data

(1) 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, to empower its competent authorities to:

a) collect or record through the application of technical means on the territory of that Party, and
b) compel a service provider, within its existing technical capability:

i) to collect or record through the application of technical means on the territory of that Party, or
ii) to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

(3) Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

(4) The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

This includes files downloaded from websites or file-sharing systems, e-mails sent or received by the offender and chat conversations.

[186] One possibility to prevent law enforcement agencies to analyse the content exchanged between two suspects is the use of encryption technology. Regarding the functioning of encryption procedures see: *Singh*; The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography, 2006; *D'Agapeyen*, Codes and Ciphers – A History of Cryptography, 2006; An Overview of the History of Cryptology – available at: http://www.cse-cst.gc.ca/documents/about-cse/museum.pdf.