Project on Cybercrime
www.coe.int/cybercrime

Economic Crime Division
Directorate General of
Human Rights and Legal Affairs
Strasbourg, France

Version 31 March 2010

Cybercrime training for judges:

Training manual (draft)

The initial version of this manual hass been prepared by Dr. Marco Gercke (Germany) for the Economic Crime Division of the Council of Europe (Directorate General of Human Rights and Legal Affairs) within the framework of the Project on Cybercrime. Inputs have also been received from Nigel Jones (Technology Risk Limited, UK) Fredesvinda Insa (CYBEX, Spain), Jan Spoenle (Max-Planck Institute, Freiburg, Germany) and other experts. It has furthermore been reviewed in connection with the PROSECO project of the European Commission and the Council of Europe on judicial networking in South-eastern Europe (www.coe.int/economiccrime).

Contact

Alexander Seger
Economic Crime Division
Council of Europe
Strasbourg, France
Tel +33 3 9021 4506
Tel +33 3 9021 5650
Alexander.seger@coe.int

Contents

1 Introduction: how to use this manual

The purpose of this manual is to facilitate the organisation of basic training courses for judges in cybercrime matters.

In recent years, societies worldwide have made tremendous advances towards becoming information societies. Information and communication technologies (ICT) now permeate almost all aspects of people's life. The increasing reliance and thus dependency on ICT makes societies vulnerable to threats such as cybercrime, that is crime committed against or through computer data and systems.

While in many countries, law enforcement authorities have been able to strengthen their capacities to investigate cybercrime and secure electronic evidence, this seems to have been less the case for judges who nevertheless play an essential role in the criminal justice process.

It is therefore required that particular efforts are undertaken to train judges and provide them with the necessary knowledge to adjudicate cases of cybercrime, or other cases involving electronic evidence.

This manual is designed to provide the material for a basic, introductory training course which should last for a minimum of two days. Obviously, it is possible to reduce or omit some of the topics and organise a one-day training course, or to expand it to one week or more by exploiting other materials referred to in the footnotes.

The structure of this manual follows the structure of the proposed course:

- Chapter 2 provides an introduction to the phenomenon of cybercrime and the challenges it poses, in particular for judges. It will furthermore introduce the "Budapest" Convention on Cybercrime of the Council of Europe which is the primary international standard ensuring a harmonisation of cybercrime legislation around the globe.

- Chapter 3 is to provide judges with a basic understanding of information technologies.

- Chapter 4 shows how the different types of conduct that make up cybercrime are defined as criminal offences. This chapter is very much based on the provisions of the Convention on Cybercrime, but it is important during a training course to relate these to the actual provisions under the respective national legislation.

- Chapter 5 offers a basic introduction to computer forensics and the question of electronic evidence.

- Chapter 6 outlines the procedural law measures that are at the disposal of criminal justice authorities in order to investigate cybercrime cases and to secure volatile electronic evidence in an efficient manner.

- Chapter 7 is about international co-operation. Cybercrime is the most transnational of all crime and cannot be addressed without efficient international co-operation. Judges play an important role in making such co-operation possible.

The appendix provides case examples that can be used to illustrate the issues dealt with in other chapters as well as a glossary of terms.

By the end of this training course judges should be able to understand why cybercrime is an important concern, what substantive and procedural laws can be applied, and why often urgent and efficient measures as well as extensive international co-operation are necessary.

Cybercrime training for judges: a typical module to provide basic training (duration: minimum 2 days, up to 5 days)

Course objective	By the end of the course judges and prosecutors should have basic knowledge of what are cybercrime and electronic evidence, how judges and prosecutors can deal with them, what substantive and procedural laws as well as technologies can be applied, and how urgent and efficient measures as well as extensive international co-operation can be taken
Session 1	About cybercrime
	➢ Why worry about cybercrime? ➢ What is cybercrime? ➢ Challenges for judges and prosecutors ➢ National law and international standards
Session 2	Technology
	➢ Functioning of the internet (basic notions) ➢ Glossary of terms ➢ Protocols
Session 3	Cybercrime as a criminal offence in domestic legislation
	➢ Offences against computer data and systems ➢ Computer-related fraud and forgery ➢ Content-related offences (child pornography, xenophobia, racism) ➢ Intellectual property-related offences ➢ Court decision/case law
Session 4	Electronic evidence
	➢ About electronic evidence: definitions and characteristics ➢ Requirements of electronic evidence ➢ Computer Forensics
Session 5	Procedural law/investigative measures
	➢ Jurisdiction and territorial competencies ➢ Expedited preservation of computer data ➢ Production orders/warrants ➢ Search and seizure of computer data ➢ The interception of traffic and content data ➢ Safeguards
Session 6	Interaction with the private sector
Session 7	International co-operation
	➢ The Convention on Cybercrime as a framework for international co-operation ➢ General principles ➢ Provisional measures and the role of 24/7 points of contact ➢ Mutual legal assistance and the role of competent authorities
Session 8	Evaluation and conclusion
Logistics and materials	The training could be provided online or in classroom. If provided in classroom: ➢ Training room with a PC and projector for presentations is sufficient (as this course does not include practical exercises such as the demonstration of forensic software or investigative techniques, a computer laboratory is not

	required) ➢ Relevant extracts of domestic substantive and procedural legislation ➢ Budapest Convention on Cybercrime including explanatory report ➢ Reader with glossary of terms and other background information ➢ If lectures are provided in a foreign language, interpretation should be foreseen and materials should be translated.

Cybercrime and electronic evidence training - a typical module for advanced knowledge (duration: minimum 2 days, up to 5 days)

Course objective	By the end of the course judges and prosecutors should have advanced knowledge that can be applied in practice on the functioning of computers and networks, what is cybercrime, cybercrime legislation, jurisdiction, investigative means and electronic evidence, and international cooperation
Session 1	Computers and networks
	➢ Glossary of computer and cybercrime terms ➢ Functioning of the ICTs/Internet infrastructure - Protocols and technology - How computers communicate - IP Investigation and electronic evidence -numbers and computer names - Role of service providers ➢ Information on the internet - Gathering of information - Use of (hidden) internet databases ➢ Profiles of social groups - Manners of communication - Manners of anonymity ➢ Detection/identification of the location and identity of computers, companies and persons on the internet
Session 2	Cybercrime and security risks
	➢ Trends in cybercrime ➢ Typologies: Particular types and techniques of cybercrime (eg phishing, botnets and other malware, child pornography) ➢ How criminals use information and communication technologies ➢ Offenders ➢ Impact of cybercrime ➢ How to enhance the security of ICTs ➢ Practical examples and simulations
Session 3	Cybercrime legislation: Substantive criminal law
	➢ Offences against computer data and systems ➢ Computer-related fraud and forgery ➢ Content-related offences (child pornography, hate crime) ➢ Intellectual property-related offences ➢ Court decision/case law
Session 4	Investigation and electronic evidence
	➢ Electronic evidence - Traces/footprints on computers, the internet, digital communication - Steps to search, seize and preserve electronic evidence - Features of forensic software - Identifying suspects - Following criminal money - Safeguards and conditions - Case management/preparation - Presenting electronic evidence in court ➢ Organisation of law enforcement with respect to cybercrime/electronic

	evidence ➢ Case studies
Session 5	Cybercrime legislation: procedural law
	➢ Expedited preservation of computer data ➢ Production orders ➢ Search and seizure of computer data ➢ The interception of traffic and content data ➢ Safeguards ➢ Interaction with internet service providers/private sector ➢ Case studies
Session 6	Jurisdiction and territorial competencies
	➢ General principles ➢ Cybercrime jurisdiction - challenges ➢ The jurisdiction provisions in the Convention on Cybercrime ➢ Case studies
Session 7	International co-operation
	➢ The Convention on Cybercrime as a framework for international co-operation ➢ General principles ➢ Provisional measures, the role of 24/7 points of contact and police co-operation ➢ Mutual legal assistance and the role of competent authorities ➢ Case studies
Session 8	Evaluation and conclusions
Logistics and materials	The training could be provided online or in classroom. If provided in classroom: ➢ Training room with a PC and projector for presentations ➢ It would be useful that trainees have a computer with internet access (but this is not a condition) ➢ Relevant extracts of domestic substantive and procedural legislation ➢ Budapest Convention on Cybercrime including explanatory report ➢ Reader with glossary of terms and other background information ➢ If lectures are provided in a foreign language, interpretation should be foreseen and materials should be translated.

2 About cybercrime

By the end of the session participants should be able to understand:

- why cybercrime should be of concern to judges
- what conduct is defined as cybercrime (typology)
- the particular challenges that cybercrime poses to judges
- why national legislation should be harmonised with international standards, that is, the Convention on Cybercrime

2.1 Why has cybercrime become an issue?

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 characterised 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 Internet access.[4] In many regions of the world, such access to information and the ability to communicate have fostered democracy, the protection of human rights and the rule of law.

These opportunities favour 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] It is not just individuals but also business which benefits from the emerging use of the Internet and from information and communication technologies (ICTs) in general. They can offer goods and services in a global environment with little financial investment.[7]

Similarly, the private life of people increasingly involves computer systems and Internet-based services. People use ICTs to develop and share their ideas, produce films, store pictures and documents and communicate with others.

---

[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 Co-operation 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.

The continuing development of ICTs has not only enhanced the possibilities of private users and businesses but also enabled offenders to target the related technology and services. Such offences range from attacks against e-commerce platforms and critical infrastructure, to obtaining identity-related information from private computers or company databases. There are therefore good reasons to argue that the security of ICTs and the protection of the confidentiality, integrity and availability of computer data and systems are at the same time protecting privacy, the freedom of expression and other fundamental rights.

In short, as societies become more dependent on ICTs, the vulnerability of society as well as the need for a response to the related threat increase. An essential element of a strategy to address the threats is the development and enforcement of cybercrime legislation. Judges play an important role in this.

2.2 What is cybercrime?

There are different views as to what exactly is cybercrime[8], the basic question being whether it comprises only offences against computer data and systems (narrow sense) or also offences committed with the help of computer data and systems (wider sense).[9] The drafters of the Convention on Cybercrime decided to include both and to define cybercrime through a set of four categories of offences:

1. Offences against the confidentiality, integrity and availability of computer data and systems
2. Computer-related offences
3. Content-related offences
4. Offences related to intellectual property rights and similar rights.

2.2.1 Offences against the confidentiality, integrity and availability of computer data and systems ("CIA offences")

This category is about cybercrime in the narrow sense and comprises offences targeting computer data and systems:

- Illegal access to a computer system. This includes one of the oldest computer crimes, namely, hacking or circumventing a password or other protection mechanism in order to access a system or data without authorisation.[10]

- Illegal interception. This offence corresponds with the unauthorised interception of a non-public communication outside computer networks – for example, the interception of phone conversations. With the increasing use of e-mail in general and wireless Internet access[11], often non-secured and unencrypted, the opportunities for illegal interception multiply.

---

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

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

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

[11] Regarding the difficulties in Cybercrime investigations that include wireless networks, see *Kang*, "Wireless Network Security – Yet another hurdle in fighting Cybercrime" " in Cybercrime & Security, IIA-2; *Urbas/Krone*, Mobile and wireless technologies: security and risk factors,

- Data interference. Like illegal access attempts to destroy or alter data by inserting malware such as viruses[12] or worms[13] are among the most traditional cybercrimes. Data on a computer can also be manipulated to create backdoors through which the computer can be accessed or controlled from outside. Alternatively, rootkits can be installed to conceal that the computer has been compromised, or spyware[14] or key loggers[15] can be installed which record the key strokes of users (for example when typing passwords or pin numbers) and send this information to criminals.

- System interference. The insertion of malware into a computer system may not only affect data but the functioning of a computer system on the whole. A form of system interference is a Denial-of-Service attack,[16] where a massive number of requests are sent to a computer system in order to hinder its operation. Often such requests are sent from a large number of individual computers (distributed denial of service attacks - DDoS) that have been infected with malicious software that enables offenders to control and use them for attacks. Such DDoS attacks through botnets[17] are now of major concern and can be used to hinder or disable critical infrastructure.

- Misuse of devices. Criminals can rely on tools that are readily available on the Internet in order to commit cybercrime.[18] This includes tools to design computer viruses, worms or other malware, to illegally access computer systems, obtain information or destroy data or to create botnets or phishing sites. The production, sale, procurement for use, import, distribution or otherwise making available of such devices is very often a preparatory act to committing further offences.

Australian Institute of Criminology, 2006 – available at: http://www.aic.gov.au/publications/tandi2/tandi329t.html.

[12] 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

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

[14] Regarding the threat of spyware, see *Hackworth*, Spyware, Cybercrime and Security, IIA-4.

[15] Regarding the use of keyloggers see: *Sieber*, Council of Europe Organised Crime Report 2004, page 65.

[16] 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.

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

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

2.2.2 Computer-related offences: fraud and forgery

This category includes offences like computer-related forgery and computer-related fraud.

Similar to forgery in the real world, information and communication technology offers multiple opportunities to manipulate computer data so that unauthentic data seem genuine and authentic and are used for legal purposes. ICTs also multiply the opportunities for fraud - that is, the loss of property of a person and economic benefits for criminals through the manipulation of computer data or interference with the functioning of a computer system.[19]

In fact, recent years have seen a shift in the threat landscape from broad, mass, multi-purpose attacks, to specific attacks on specific users, groups, organisations or industries, increasingly for economic criminal purposes. These include:

- Credit card fraud[20]
- Advance fee fraud[21]
- Internet marketing and retail fraud
- Auction fraud[22] and stock market manipulation

2.2.3 Content-related offences: child pornography, racism and xenophobia

While the internet offers unique opportunities for creativity and the expression of different opinions, it also creates also opportunities for misuse. The internet has become a key platform for the trading of child pornography, that is, for pornographic materials that visually depict a minor (or a person appearing to be a minor or a realistic image of a person appearing to be a minor) engaged in sexually explicit conduct.[23] The acts related to child pornography range from the production and dissemination to the possession of related material.

Illegal content available on the Internet is not limited to child pornography. Radical groups use mass communication systems such as the Internet to spread

[19] For details see below: Chapter

[20] Regarding the extend of credit card fraud see Consumer Fraud and Identity Theft Complain Data, January – December 2005, Federal Trade Commission, 2006, page 3 –available at: www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf.

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

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

[23] Regarding the means of distribution, see: *Wortley/Smallbone*, Child Pornography on the Internet, page 10 et seq. - available at: http://www.cops.usdoj.gov/mime/open.pdf?Item=1729.

propaganda.[24] The number of websites offering racist content and hate speech has constantly increased in the last years.[25]

The Council of Europe addresses this through the a protocol to the Convention on Cybercrime on "Xenophobia and Racisms committed through Computer Systems" (CETS 189).[26]

2.2.4 Offences related to intellectual property rights and similar rights

The digitalisation of ways to distribute music, videos and books has opened the door to new forms of copyright violations. File-sharing systems, which enable users to share files,[27] allow users easy access to thousands of copyright protected files.[28]

2.2.5 Combinations of offences

Phishing and identity theft

Not all offences can be linked to one of the four categories, as they combine conduct under more than one category. One example is "phishing".[29] "Phishing" describes acts that are carried out to make victims disclose personal/secret information.[30] In the most common e-mail-based phishing scams the offenders contact the victims via e-mail, pretending to be a legitimate company, and seeking to disclose information that the offenders can then use to commit further offences. Those scams can include crimes such as computer-related forgery, computer-related fraud and trademark violations.

A related example is "identity theft".[31] This term describes the act of obtaining, transferring or using identity-related information of a third person, or even a synthetic

---

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

[25] *Sieber*, "Council of Europe Organised Crime Report 2004", page 138.

[26] See www.coe.int/cybercrime for a link to the Protocol.

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

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

[29] 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

[30] 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.

[31] For an overview about identity theft see: *Chawki/Abdel Wahab*, Identity Theft in Cyberspace: Issues and Solutions, Lex Electronica, Vol. 11, No. 1, 2006; *Ceaton*, The Cultural Phenomenon of Identity Theft and the Domestication of the World Wide Web, Bulletin of Science Technology Society, 2007, Vol. 27, 2008, page 11 et seq.; *Elston/Stein*, International Co-operation in On-Online Identity Theft Investigations: A Hopeful Future but a Frustrating Present, available at: http://www.isrcl.org/Papers/Elston%20and%20Stein.pdf; *Emigh*, Online Identity Theft: Phishing Technologies, Chokepoints and Countermeasures, ITTC Report on Online Identity Theft Technology and Countermeasures, 2005; *Halperin*, Identity as an Emerging Field of Study, Datenschutz und Datensicherheit, 2006, page 533 et seq; *Koops/Leenes*, Identity Theft, Identity

identity with the intention to use it in a criminal context, as well as the criminal acts carried out by using the identity (such as fraud).[32]

Organising for cybercrime

ICTs certainly facilitate the activities of organised criminal groups. However, in addition the nature of cybercrime has been changing in recent years. The focus of cybercrime has shifted from disorganised hacking to generating criminal proceeds, and this shift is going hand in hand with cybercrime being increasingly organised.

Organising for cybercrime may include elements of traditional organised crime or economic crime in combination with computer-related fraud and forgery, offences related to intellectual property and related rights, data and system interference (such as use of botnets) or other conduct.

- As economic crime is already a primary activity of organised crime, ICTs further facilitate offences such as credit card, "pump-and-dump" schemes and other kinds of fraud, money laundering, counterfeiting, or fraud schemes based on identity theft but also modern forms of traditional crimes such as electronic bank robberies or cyber-extortion.
- Depersonalisation of contacts, ease of access and rapidity of electronic transactions make ICT an attractive tool for money laundering. Virtual casinos, auctions, smart cards, online banking, or the possibility to purchase and sell shares, bonds and futures online offer ample opportunities for money laundering.
- Organised crime exploits the vulnerability of societies, public institutions, business sector and of individuals using the internet. Not only corporations engaged in e-commerce and business-to-business operations, but also individuals using online banking or participating in e-commerce become victims of electronic theft and phishing. Victims include children as the most vulnerable group of society.
- ICT offer anonymity, facilitate the logistics and reduce the risks for organised criminals to be prosecuted. It permits remote controlled operations, covert activities, transnational operations, networking and encrypted communication.
- ICT are a tool for global outreach and search for potential victims. An example is the Nigerian-fraud schemes which have proliferated through the internet and under which people all over the world are lured into making advance payments for dubious money transfer schemes.
- Botnets through which large numbers of computers can be turned into zombies and controlled remotely by a command and control servers are considered one of the main tools of organised criminals.

It can also be argued that ICT will change the shape of organised crime, that is, the way people organise themselves to carry out crimes. Cybercrime does not require control over a geographical territory, requires less personal contacts and thus less relationships based on trust and enforcement of discipline between criminals, in short less need for formal organisation. The classical hierarchical structures of organised

---

Fraud and/or Identity-related Crime, Datenschutz und Datensicherheit, 2006, page 553 et seq.; *Levi,* Combating Identity and Other Forms of Payment Fraud in the UK: An Analytical History, published in McNally/Newman, Perspectives on Identity Theft; *Van der Meulen,* The Challenge of Countering Identity Theft: Recent Developments in the United States, the United Kingdom and the European Union, Report commissioned by the National Infrastructure Cybercrime Programme (NICC); *Gercke*, Internet-related Identity Theft, 2007 – available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_co-operation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

[32] For an overview about the different definition 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_co-operation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

crime groups may even be unsuitable for organised crime on the internet. ICT may favour those organisations which are already based on flat-structured networking. ICT may also change the characteristics of offenders. In the real world legal businessmen engage in organised forms of economic crime; and, *modus modendi,* the opportunities offered by ICT may tempt legal commercial entities to organise for cybercrime, that is, become organised cyber criminals.

Terrorist use of the internet

Another area of cybercrime that combines offences from different categories is the terrorist use of ICT. While the term "cyberterrorism" is somewhat controversial, it is clear that terrorist use the internet and ICTs in general for their activities. For example:

- Propaganda: While in 1998 only 12 foreign terrorist organisations listed by the US State Department maintained websites,[33] in 2004 the United States Institute of Peace reported that nearly all terrorist organisations maintain websites – among them Hamas, Hezbollah, PKK and Al Qaida.[34] Apart from maintaining websites, terrorists have also started to use online communities to distribute video messages and propaganda.[35]

- Collecting information: Information that can be helpful to identify possible targets for terrorist attacks is available online.[36] Today high resolution satellite pictures, that years ago were only available to very few military institutions in the world, are available for free on various Internet services.[37] In addition, instructions on how to build bombs and even virtual training camps that provide instructions on the use of weapons in an e-learning approach were discovered.[38] Furthermore, sensitive or confidential information that is not adequately protected from search-robots and can be accessed via search engines.[39] In 2003, the US Department of Defence was informed about a training manual linked to Al Qaeda providing information on how to use public sources to find out details about potential targets.[40]

- Providing information: Online services can be used to spread training material such as instructions on the use of weapons and the selection of targets. Such material is

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

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

[35] Regarding the use of YouTube by terrorist organisations, see Heise Online News, 11 October 2006, available at http://www.heise.de/newsticker/meldung/79311; *Staud* in Sueddeutsche Zeitung, 05.10.2006.

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

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

[38] For further reference see *Gercke*, 'The Challenge of Fighting Cybercrime', Multimedia und Recht, 2008, page 292.

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

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

available on a large scale from online sources.[41] In 2008 an Internet server that provided a basis for the exchange of training material, as well as communication among terrorists, was discovered.[42] Different websites were reported to be operated by terrorist organisations to co-ordinate activities.[43]

- Communication: After the 9/11 attacks it was reported that terrorists used e-mail communication within the co-ordination of their attacks.[44] The press reported about the exchange of detailed instructions about the targets and the number of attackers via e-mail.[45]

- Terrorist financing: A significant number of the active terrorist organisations depend on financial resources they receive from third parties. Tracing back these financial transactions has become one of the major tasks in the fight against terrorism after the 9/11 attacks. One of the main difficulties in this respect is the fact that the financial resources required to carry out attacks are not necessary huge.[46] There are two ways in which Internet services can be used for terrorist financing:
  - terrorist organisations can make use of electronic payment systems to enable online donations[47] or at least publish information how to donate on websites;[48]
  - to avoid discovery terrorist organisations try to conceal their activities by involving non-suspicious players such as charity organisations. Another (Internet-related) domain is the operation of fake web-shops.

- Training for real world attacks: Reports point out that terrorists have started to use online games to prepare for situations in a real-world attack.[49] There are

[41] *Brunst* in *Sieber/Brunst*, 'Cyberterrorism – the use of the Internet for terrorist purposes', Council of Europe Publication, 2007; US Homeland Security Advisory Council, Report of the Future of Terrorism Task Force, January 2008, page 5; *Stenersen*, 'The Internet: A Virtual Training Camp?, Terrorism and Political Violence, 2008, page 215 et seq.

[42] *Musharbash*, 'Bin Ladens Intranet', Der Spiegel, Vol. 39, 2008, page 127.

[43] *Weimann*, 'How Modern Terrorism Uses the Internet', 116 Special Report of the US Institute of Peace, 2004, page 10.

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

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

[46] The Commission analysing the 9/11 attacks calculated that the costs for the attack could have been between USD 400,000 and 500,000. See 9/11 Commission Report, Final Report of the National Commission on Terrorist Attacks Upon the United States, page 187. Taking into account the duration of the preparation and the number of people involved the cost per person have been relatively small. Regarding the related challenges see as well *Weiss*, CRS Report for Congress, 'Terrorist Financing: The 9/11 Commission Recommendation', page 4.

[47] See in this context *Crilley*, 'Information Warfare: New Battlefields – Terrorists, Propaganda and the Internet', Aslib Proceedings, Vol. 53, No. 7 (2001), page 253.

[48] *Weimann* in USIP Report, 'How Terrorists Use the Internet', 2004, page 7; See *Conway*, Terrorist Use the Internet and Fighting Back, Information and Security, 2006, page 4.

[49] See US Commission on Security and Co-operation in Europe Briefing, 15.05.2008, available at http://csce.gov/index.cfm?FuseAction=ContentRecords.
ViewTranscript&ContentRecord_id=426&ContentType=H,B&ContentRecord
Type=B&CFID=18849146&CFTOKEN=53; O'Brian, Virtual Terrorists, The Australian, 31.07.2007, available at http://www.theaustralian.news.com.au/story/
0,25197,22161037-28737,00.html;

various different online games available that simulate the real world. The user of such games can make use of characters (avatar) to act in this virtual world. Theoretically those online games could be used to simulate attacks, but it is not yet certain to what extent such online games are already involved in this kind of activity.[50]

- Internet-related attacks against critical infrastructure: Critical (information) infrastructure could become a target for terrorists. Critical infrastructure is widely recognised as a potential target for terrorist attacks as it is by definition vital for the stability of a state.[51] Infrastructure is considered to be frail if its incapacity or destruction would have a debilitating impact on the defence or economic security of a state.[52] This concerns in particular electrical power systems, telecommunication systems, gas and oil storage and transportation, banking and finance, transportation, water supply systems and emergency services. The degree of civil disturbance caused by the disruption of services by Hurricane Katrina highlights the dependence of society on the availability of those services.[53]

  The growing reliance on information technology makes critical infrastructure more vulnerable to attacks.[54] This is especially the case with regard to attacks against interconnected systems that are linked by computer and communication networks.[55] Even short interruptions to services could cause huge financial damages to e-commerce businesses – not only for civil services, but also for military infrastructure and services.[56] While carrying out the attack, the offenders can use the means of anonymous communication and encryption technology to hide their identity.[57]

The "terrorist use of the internet" thus comprises a combination of offences. Full implementation of the Convention on Cybercrime would allow countries to criminalise attacks against ICTs, to secure evidence on computer systems used by terrorists and to co-operate internationally. The Council of Europe Convention for the Prevention of Terrorisms[58] in addition provides specific measures related to recruitment and training of terrorists and the incitement to terrorism.

---

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

[51] *Brunst* in *Sieber/Brunst*, 'Cyberterrorism – The Use of the Internet for Terrorist Purposes', Council of Europe Publication, 2007.

[52] US Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138.

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

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

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

[56] *Shimeall/Williams/Dunlevy*, Countering Cyber War, NATO Review, winter 2001/2002, available at http://www.cert.org/archive/pdf/counter_cyberwar.pdf.

[57] CERT Research 2006 Annual Report', page 7 et seqq., available at http://www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

[58] Convention for the Prevention of Terrorism (CETS 198) http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=196&CM=8&DF=3/2/2009&CL=ENG

2.3 Challenges for judges

2.3.1 The role of judges

Judges play a crucial role in the fight against cybercrime. Without their contribution offenders cannot be convicted. There is a number of specific challenges related to the role of judges in cybercrime investigations:

- Although some cybercrime offences – such as e-mail fraud - might at least in some countries be covered by traditional criminal law provisions, there are offences that require special provisions. With regard to such new provisions, it is necessary to provide judges with background information related to the interpretation and application.

- One of the main difficulties judges are facing is related to the time of their involvement in the investigation. Apart from cases where the national law requires a court order[59] for specific investigations, the judges are in general only involved in the last phase of the case – the court proceedings. As described in more detail below, cybercrime cases are to a large extent dependent on the availability of electronic evidence.[60] IP-addresses can help the investigators to identify the connection used to send out illegal content, and log-files on the suspect's computer might be useful to prove which user committed the crime. Such data are highly ephemeral and therefore need to be collected in due time. By the time that judges become involved there is in general very little chance for the collection of further evidence. If a judge realises that important evidence is missing it is very unlikely that at that point it is possible to correct mistakes made during earlier phases of an investigation. With regard to cybercrime-related cases, the judge therefore depends heavily on the quality of previous investigations.

- Judges – and in cases where a jury is involved the jurors – need to be able to evaluate the significance of the electronic evidence without having the possibility to participate in the process of collecting the evidence. Without being an expert in computer forensics it can be difficult to go through the evaluation process. Although the evaluation of the evidence can be partly delegated to court experts and expert witnesses, a basic understanding of the fundamental principles of computer forensics is a key requirement for judges dealing with cybercrime cases. Providing this kind of training is easier in countries[61] that have established specialised courts chambers dealing exclusively with cybercrime than in countries where potentially every judge could become responsible for such a case.

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

[60] See below: Chapter 4.

[61] Serbian Law on the Organisation and Jurisdiction of Government Authorities in Suppression of High Technological Crimes.

2.3.2 Volatile nature or electronic evidence

The transfer of an e-mail with an attachment containing xenophobic material or the downloading of a child pornography picture in general only takes seconds. The information that the law enforcement agencies need to trace back and identify the offender is – if no data retention obligations are in place - often deleted shortly after the finalisation of the transfer process.[62] This leaves a very short time frame for investigations.[63]

2.3.3 Number of users

Currently more than 1 billion people worldwide use the Internet[64] and it is likely that this number will increase continuously in the coming years. The number of possible offenders is significant due to the international dimension of the network. 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 carries the question of how to identify web pages with illegal content within billions of web pages available in the Internet? This illustrates how difficult it is for investigating authorities to fight cybercrime.

2.3.4 Co-operation between law enforcement authorities and private businesses

An effective fight against cybercrime is not only dependent on the availability of sufficient legislation; the relationship between law enforcement agencies and private businesses such as Internet Service Provider (ISP) is considered another essential element. [65] 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 ISPs.[66] The guidelines were based on a study that analysed the existing structure of co-operation.[67] During the 2008 Council of Europe Octopus Interface Conference[68] the guidelines were adopted as an informal, non-binding tool.[69]

---

[62] *Gercke*, DUD 2003, 477 et seq.; *Lipson*, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

[63] *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", CRi 2006, 142.

[64] According to „Internet World Stats" more than1,15 Billion people are using the Internet by 2007 (the statistic are available at: http://www.internetworldstats.com/stats.htm).

[65] See Guidelines for the co-operation of law enforcement and internet service providers against cybercrime, No.3.

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

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

[68] The program of the conference is available at: http://www.coe.int/t/dg1/legalco-operation/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/legalco-operation/economiccrime/cybercrime/cy%20activity%20Interface2008/567_IF08-d-concl1c.pdf.

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

2.3.5 International dimension

Data transfer processes very often affect more than one country.[70] This is due to the design of the network, as well as the fact that protocols ensure that successful transmissions can take place even if direct lines are temporarily blocked.[71] In addition, a large number of Internet services (like for example hosting services) are offered by companies that are based abroad.[72]

In cases where the offender is not based in the same country where the victim is located, the investigation requires the co-operation of law enforcement agencies in all countries through which data flow.[73] Transnational investigations without the consent of the competent authorities in the countries involved are difficult for the principle of national sovereignty. This principle does not in general allow one country to carry out investigations within the territory of another country without a permission of the local authorities.[74] Thus investigations required the support of the authorities of all countries involved.

Given that in most cases there is only a very short time gap available in which successful investigations can take place and electronic evidence secured, the application of traditional mutual legal assistance regimes are insufficient. The Convention on Cybercrime foresees expedited measures to help preserve data, among others with the help of a 24/7 network of contact points.

2.3.6 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 located. This independence of place of action and the location of the victim can cause difficulties with regard to cybercrime investigations. Offenders can try to avoid criminal proceedings by acting from countries with weak cybercrime legislation.[75] An effective fight against cybercrime therefore requires preventing "safe havens" which enable offenders to hide their activities and operate with impunity.[76]

---

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

[71] 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.

[72] 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.

[73] 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

[74] 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.

[75] 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.

[76] The issue was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out: "States should ensure that their laws and practice eliminate safe

An example for difficulties resulting from safe havens was the "Love Bug" computer worm that spread in 2000.[77] The computer worm infected millions of computer systems worldwide.[78] Intensive investigations led to the suspect in the Philippines. Due to the fact that the development and spreading of malicious software was at that time not sufficiently criminalised in the Philippines, the local investigations were seriously hindered.[79]

2.3.7 Resources

One of the main challenges for law enforcement agencies is the fact that a number of organised crime groups have access to a significant number of computer systems that they can use to carry out automated attacks.[80] An example for the use of a large number of computer systems to carry out an attack was the successful attack against government websites in Estonia.[81] Analyses of the attacks point out that the attacks involved thousands of computers that were part of a so called "botnet".[82]

In contrast to criminals that do dispose of considerable means and do not need to respect borders, the resources of judges and other criminal justice authorities are much more limited.

An important question is how judges and other law enforcement and criminal justice authorities can be sufficiently trained and equipped to meet the challenge of cybercrime.

2.3.8 Protection of fundamental rights

Freedom of speech[83] and privacy (including the protection of personal data) are two issues that are in the focus of the discussion about the protection of Internet users.[84]

---

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".

[77] 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.

[78] 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.

[79] 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;

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

[81] 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.

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

[83] 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

It can be assumed that the vast majority of people use ICTs for perfectly legitimate purposes. It is therefore essential to balance the need for efficient and effective law enforcement and the fundamental rights of users. In the Convention on Cybercrime this is reflected in Article 15:

> Article 15 – Conditions and safeguards
>
> 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.
>
> 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.
>
> 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

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 when investigating, prosecuting or adjudicating cybercrime. Judges play a most critical part in this respect.

In February 2008,[85] the German Constitutional Court stated that the confidentiality, integrity and availability of computer systems are protected by the German Constitution. This underlines the importance of safeguards as new investigate tools are developed.

At the same time, if computer systems contain the core of the private life of citizens, measures to protect such systems and effective criminal justice measures will be major contributions to protect the fundamental rights of citizens. In this sense, security and the rights of citizens go hand in hand.

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.

[84] 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.

[85] BVerfG, 1 BvR 370/07 vom 27.2.2008.

2.4 National law and international standards: the Convention on Cybercrime

2.4.1 The criminal law response at the national level

As mentioned above, an adequate legislation is the foundation for successful investigation, prosecution and adjudication of cybercrime.

At a national level, the criminal law response should basically consist of the following elements:

- Criminalisation of certain conduct (substantive criminal law)
- Development of procedural instruments that enable law enforcement agencies to carry out investigations
- Incorporate means of international co-operation that enables the competent authorities to co-operate with foreign counterparts in an efficient manner.

The Convention on Cybercrime serves as a guideline that helps ensure that substantive and procedural law provisions are consistent and comprehensive as well as as harmonised between countries. For countries that are parties to the Convention it also serves as a framework for international co-operation.

As indicated earlier on, the country profiles developed by the Council of Europe's Project on Cybercrime help relate the provisions of the Convention to specific provisions in national law.

2.4.2 The Convention on Cybercrime

Background

Cybercrime is probably the most transnational crime[86], thus requiring global co-operation among law enforcement and criminal justice authorities.[87] Due to the difficulties of international co-operation on the basis of differing national standards (especially because of the "dual criminality[88]" requirement), a fundamental component of strategies to improve international co-operation is the harmonisation of national laws. More specifically, countries need to agree on common standards with regard to substantive criminal law and procedural law and in addition develop legal standards for international co-operation.

[86] Regarding the extent of transnational attacks in the most damaging cyberattacks, see: *Sofaer/Goodman*, "Cyber Crime and Security – The Transnational Dimension" in *Sofaer/Goodman*, "The Transnational Dimension of Cyber Crime and Terrorism", 2001, page 7, available at: http://media.hoover.org/documents/0817999825_1.pdf.
[87] *Gercke*, "The Slow Wake of A Global Approach Against Cybercrime", CRI 2006, 142.
[88] Regarding the dual criminality principle in international investigations see: United Nations Manual on the Prevention and Control of Computer-Related Crime, 269 – available at *http://www.uncjin.org/Documents/EighthCongress.html* (last visited: January 2008); *Schjolberg/Hubbard*, Harmonizing National Legal Approaches on Cybercrime, 2005, page 5 – available at: *www.itu.int/osg/spu/cybersecurity/ presentations/session12_schjolberg.pdf*.

The Convention on Cybercrime[89] provides a legal framework for the development of such legislation. This treaty has been developed by the Council of Europe (currently 47 member States) in co-operation with the non-member states Canada, Japan, South Africa and the United States of America and was opened for signature in 2001. It entered into force in 2004.[90] This Convention is open to any country from around the world that may seek accession.[91] For example, in February 2007 Costa Rica and Mexico, in May 2008 the Philippines and in November 2008 the Dominican Republic were invited to become a party, and a number of other countries from different regions of the world are about to seek accession. Equally important is that many countries are currently preparing new cybercrime legislation using the Convention as a model.[92]

Structure of the Convention

The treaty is structured as follows:

- Chapter I: Definitions of a computer system, computer data, service provider, traffic data

- Chapter II: Measures to be taken at the national level

  Section 1 - Substantive criminal law, that is, conduct that is to be made a criminal offence. This includes:
  - Offences against the confidentiality, integrity and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices)
  - Computer-related offences (computer-related forgery, computer-related fraud)
  - Content-related offences (child pornography, and in a separate Protocol also xenophobia and racism)
  - Infringement of copyright and related rights

  Section 2 - Procedural law, that is, measures for more effective investigations of cybercrimes. These include:
  - Procedural safeguards
  - Expedited preservation of stored computer data
  - Expedited preservation and partial disclosure of traffic data
  - Production order
  - Search and seizure of stored computer data
  - Real-time collection of traffic data

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

[90] The requirements for the Convention to come into power are regulated in Art. 36 Convention on Cybercrime.

[91] The accession process by non-members is regulated in Art. 37 Convention on Cybercrime.

[92] Regarding the model law character of the Convention and the use by non-signatory countries see: *Gercke*, National, Regional and International Aproaches in the Fight Against Cybercrime, CRi 2008, page 7 et seq.

- Interception of content data

Section 3 - Jurisdiction

- Chapter III: International co-operation

  Section 1 - General principles of co-operation, that is, general principles on international co-operation, principles related to extradition, principles related to mutual legal assistance, spontaneous information, mutual legal assistance in the absence of applicable international instruments, and confidentiality and limitation on use

  Section 2 - Specific provisions for more effective co-operation. These permit parties to the Convention to apply procedural tools also internationally. Provisions include the expedited preservation of stored computer data, the expedited disclosure of preserved computer data, mutual assistance regarding accessing stored computer data, trans-border access to stored computer data (public/with consent), mutual assistance in the real-time collection of traffic data, and mutual assistance regarding interception of content data. This Section also provides for the creation of a network of contact points which are available on a 24/7 basis to facilitate rapid co-operation.

- Chapter IV: Final provisions. This chapter is of particular interest to non-European countries as it provides for the accession on non-member States to the Convention.

The different provisions of the Convention will be discussed in detail in one of the following chapters which will focus on the types of conduct that constitute criminal offences.

3 Technology for judges

3.1 Introduction

This chapter is intended to provide training developers with a framework for developing training material to be delivered as part of a wider programme. It cannot be comprehensive as technology changes so rapidly that any detailed technical specifications would be out of date almost as soon as the document is published. Ensuring that Judges have sufficient understanding of technical issues as they relate to matters before them is essential to the fair running of any judicial system. This chapter provides an overview of the relevant aspects of technology and its relevance to the judiciary.

This chapter provides information about technology that will be encountered by Judges during their work and which is used by criminals to commit crime and law enforcement to detect it.

3.2 How Computers Work

By the end of the session participants should be able to:
- List the component parts of a computer system
- Explain how data is stored on computer systems
- Identify different computer operating systems

In order for Judges to fully understand the impact of technology on crime, it is necessary for them to gain an understanding of the fundamentals of how the technology they are presented with functions. In particular, in cases involving digital forensics in its broadest sense, this knowledge will provide context and enable informed decisions to be made.

3.2.1 Computer components

A computer consists of many components and it is relevant for judges to understand the names and functions of these components as they will be referred to in statements and evidence. A brief explanation is provided of each component as follows:

- Motherboard - A motherboard is also known as the main board or system board of the computer. The motherboard is the central circuit board of a computer. All other components and peripherals plug into it. The job of the motherboard is to relay information between them all. The motherboard houses the BIOS (Basic Input/Output System), which is the simple software run by a computer when initially turned on. Other components attach directly to it, such as the memory, CPU (Central Processing Unit), graphics card, sound card, hard-drive, disk drives, along with various external ports and peripherals.

- Power Supply – The **P**ower **S**upply **U**nit (PSU) in a computer regulates and delivers the power to the components housed in the case. Standard power supplies turn the incoming 110V **or** 220V AC (Alternating Current) into various DC (Direct Current) voltages suitable for powering the computer's components. Power supplies have a certain power output specified in Watts, a standard power supply would typically be able to deliver around 350 Watts. The more components there

are in a PC the greater the power required from the power supply.

- CMOS and BIOS - CMOS and BIOS are often used interchangeably; you can think of the BIOS as software, and CMOS as the hardware running it. Abbreviated from Complementary Metal Oxide Semiconductor, CMOS is usually pronounced "*see*-moss". CMOS is the hardware in a computer that performs very low-level functions and very basic computer start routines. The CMOS does things like maintain a computer's clock, and provides the interface to the rest of the computer hardware for the BIOS to do its job. It requires very little power to operate.

- Abbreviated from Basic Input / Output System, it's usually pronounced "*bye*-oss". The BIOS is an interface that allows a user to make low-level changes to a computers motherboard, CPU, memory and other devices. The default BIOS settings are usually set just right. One of the most common changes made to the BIOS in a forensic capacity is to change the order in which the computer looks for devices to boot (start) from. Typically a forensic examiner may use software on a Compact Disk (CD) and will change the BIOS so that the computer starts from the CD and not from the hard disk as this would alter data just by accessing and starting from the hard disk.

- Expansion Ports/Slots – these are the slots on the back of the computer where you can connect sound cards, video cards, wireless adapters, etc.

- Central Processing Units (CPU's) - CPU stands for the Central Processing Unit of a computer system. People often mistake the case or chassis of a computer as the CPU. However, the CPU is an internal component of the computer. It cannot be seen from the outside of the system. The first CPUs were used in the early 1960s. With the introduction of the integrated circuit in the late 1970s, it became possible for smaller CPUs to be manufactured as well. This helped transform computers from large, bulky devices that took up entire rooms to more manageable desktop and laptop models.

- No matter what the type of computer, the CPU works by executing a series of stored instructions known as a program. Most CPUs conform to the von Neumann architecture, which says that the CPU must fetch, decode, execute, and write back the data in a fairly rapid succession. For the layman a CPU is nothing but brain of the computer i.e as what computer actually performs is basically done with the help of CPU.

- Memory – Computer memory is technically any form of electronic data storage, although it is most commonly used to describe temporary forms of storage that can be accessed rapidly. It would be a very slow process if the CPU had to obtain data from the hard disk every time it executed an instruction; so much data is temporarily stored in temporary memory in order that it may be accessed more quickly. This type of memory is known as Random Access Memory (RAM). The CPU will request data from RAM, process it and write it back to RAM. This takes place millions of times per second. Understanding temporary memory is important in the forensic capture of data from computers as this data is not saved if the power from the computer is disconnected, as is a common feature of search and seizure of computer systems. It is now more common for Law Enforcement to attempt to capture data in RAM before disconnecting the power during computer searches. This is commonly known as "Live Data Forensics". This activity is happening more often as the amount of data that may be lost is greater than the size of the largest hard disk of only a few years ago.

- Hard Disk Drives - Most computers have at least one hard disk and many have more. Larger computers such as mainframes will typically have many hard disks. It is now common for other devices such as CCTV and music players to also have hard disks which can hold huge amounts of data. These disks have hard platters on which information is held and data can be easily deleted and rewritten, while the structure of the disk is remembered, making them viable for long periods of time. Data is stored on the surface of a platter in sectors and tracks. Tracks are concentric circles, and sectors are pie-shaped wedges on a track. Data is stored on hard disks as files which are simply a group of "bytes". Programmes are also files and these are also called by the CPU in order to be used.

- CD/DVD/Blu-Ray Disks – These disks may hold varying amount of data and are typically used to store music, video or computer files for distribution. A DVD for example is the same size as a CD and holds about 7 times as much data as a CD. A Blu-Ray disk, which may be used to store high definition content in turn currently holds more than 10 times as much as a DVD. In other words they can store more data than was possible on a hard disk only a few years ago. They all store data in a different way than hard disks and the data held on them is not as volatile as that stored on hard disks.

- Universal Serial Bus (USB) – USB connectors found on most computers allow for simple attachment of a large number of devices to the computer, such as mice, printers, external storage devices and mobile phones. It is currently the most common method of connecting external devices to computers. Historically, other connection methods such as parallel or serial ports were more problematic as there was a limit to the number of devices that could be connected at one time, and the rate of data transfer were much slower than USB. It is possible to connect up to 127 devices to a computer using USB. The ease with which USB devices can be used means that they are prominent in many digital forensic investigations.

There are many other computer components that are not dealt with in this chapter; however the most important for the purpose of the manual are included. For the purpose of developing training programmes it is recommended that components not covered here are explained, depending on the knowledge level of individuals. It would be expected that most recipients of training will understand what a keyboard and mouse are for example, but trainers should not overestimate the knowledge of individuals. Items that may be added to the list above may include: printers, scanners, webcams, modems, speakers, computer and video phones and various storage devices and network connections as well as external ports such as Firewire and USB.

In particular see http://computer.howstuffworks.com/computer-hardware-channel.htm for more detailed information about computer hardware; including photographs which will substantially increase the ease with which these concepts may be understood. Remember to obtain permission from the owners of the information if it is proposed to be used in training programmes.

3.2.2 Data Storage

It is an everyday practice for evidence to be produced in criminal and civil proceedings that emanates from computers or either digital devices such mobile phones. As technology continues to pervade society, it will become the norm for more and more devices to contain digital evidence that may be used in proceedings. We are already seeing domestic devices being examined to extract such evidence.

It is therefore vital that Judges have an understanding of the issues that impact on the integrity and admissibility of digital evidence. As a start point, it will be useful for them to appreciate how data is stored and recovered by investigators.

Electronic or digital data is stored in many forms, the most prominent and in many ways the easiest to validate is that stored on computer hard drives. Typical approaches to preservation and production of digital evidence rely on examination on devices in a static condition. In other words when a computer is switched off and data is not in a truly volatile state. Digital forensics examiners are well versed in the requirements of international and national guidelines on the handling of such evidence. One such guide titled Seizure of E-Evidence was developed with funding support from the European Commission Oisin programme and may be found at: http://www.e-evidence.info. This guide promotes the general principles by which most law enforcement work. It is important that Judges have a clear understanding of the way in which data is stored as well as how the evidence is adduced that is presented before them. This requires a fundamental understanding of the concepts of digital data, storage, retrieval and the tools and procedures used to bring that evidence into the criminal justice system. There are numerous resources open to training developers to gather information about hard disk storage to use within learning programmes. One such example may be found at: http://www.storagereview.com/hard_disk_drive_reference_guide. This generally deals with non-volatile storage such as magnetic media, optical storage media, flash memory etc.

It is now more common for evidence to be recovered from volatile sources such as Random Access Memory (RAM) or devices such as mobile phones where data is more volatile. Judges need to understand the differences in the manner in which such data is recovered and any effect on the integrity of evidence. The importance of recovering volatile data is simply that it is generally lost when a device is powered down and the opportunity to recover large amounts of valuable information that may prove to be valuable evidence has gone. The techniques used to recover this information should comply with the general principles for the preservation and recovery of such data. It is also typical for volatile data to be recovered from networked systems that cannot be shut down for a static analysis to be conducted.

3.2.3 Operating Systems

In order to function, computers and other digital devices require an operating system. An operating system is a software programme that allows the hardware to communicate with software programmes. Without an operating system the computer would not be able to function. There are different types of operating system depending on the type of computer or other digital device.

The most common operating systems in use today are commonly known under the following headings: Windows, Unix/Linux and Apple Mac. There are other systems in use particularly for other types of device such as personal digital assistants and mobile telephones. These are often cut down versions of the major systems although it is now more common for bespoke systems to be developed for some smaller devices.

Most applications developed for computers are written for specific operating systems although it is now more common for them to be available for more than one platform.

It is important that judges appreciate the importance of operating systems and are familiar with the fact that different operating systems behave in different ways. There are many references that will enable a training developer to include sufficient information about operating systems to meet the objectives set out for this section. Among these resources are: http://en.wikipedia.org/wiki/Operating_systems.

3.3 How the Internet Works

By the end of the session participants should be able to:
- Explain how the Internet has developed from its beginning to today.
- Differentiate between different Internet applications
- Identify how the various Internet applications may be used by criminals

The term INTERNET comes from the contraction of the words INTERconnected NETwork. Many criminal activities involve the use of the Internet and this includes particular types of crime such as hacking, distribution of viruses and phishing attacks as well as more traditional crimes such as fraud. In order for Judges to effectively manage such cases that appear before them, it is necessary for them to understand the fundamentals of the Internet and its applications such as the World Wide Web and email. The following provides an introduction to the subject and provides the template for a successful training module.

3.3.1 The History of the Internet

The Internet began its life as the ARPANET in the 1960's. The relevance of this information may not be immediately apparent; however, the fact that the Internet was never designed to be secure may explain why it is comparatively easy for criminals to abuse the systems. The first physical links were created in 1969 with 4 nodes being universities. The first email was sent in 1972 and the following year a new communications protocol TCP/IP was created, which now forms the basis upon which Internet communications take place. The development of the Internet as we now know it was low key in the beginning as there were disjointed separate networks, served only by limited gateways between them. This led to the application of packet switching to develop a protocol for internetworking, where multiple different networks could be joined together into a super-framework of networks.

This enabled further interconnection, which began to occur more quickly across the advanced networks of the western world, and then began to penetrate into the rest of the world. The disparity of growth between advanced nations and the developing world led to a digital divide that still exists today.

There followed the commercialisation of the Internet and the introduction of privately run Internet service providers in the 1980s. These enabled more popular access which really developed in the 1990's. The Internet has had a huge impact on commerce as well as culture. There now exists near instant communication by electronic mail (e-mail), social networking sites, text based discussion forums, and the World Wide Web. The Internet continues to grow, driven by commerce, greater amounts of online information and knowledge. The advent of Web 2.0 is upon us.

3.3.2 How the Internet functions

The Internet can be thought of as the infrastructure over which many different applications can be run simultaneously. If any part of the Internet malfunctions or is

destroyed, communication can still continue. No-one owns the Internet – no organisation, no corporation, no government. It is largely self regulated. It all uses the same connection technology.

Most modern data networks, like the Internet, are described as "connectionless" or "packet switched". Traffic is split into small packets which make their own way from sender to receiver. They do not all follow the same route and are joined together again when they reach their destination.

Most people connect to the Internet through an Internet Service Provider (ISP). These are commercial organisations that rent out space. They keep records…but for how long? There are national and international legal data protection or privacy issues that impact on how long data may be retained by ISP's. This of course has an impact on the ability of criminal justice officials to secure evidence from these sources. Connection is normally made by one of the following methods; Dial-up, Broadband (ADSL), ISDN, Cable, Wireless hotspot or Satellite.

An excellent resource for explaining the Internet is a movie called "Warriors of the Net". It is the perfect tool for introducing Internet to novice users. It helps the newcomers visualise how the Net works. The movie is 12 minutes long. It is about an IP packets journey through net past routers, firewalls and transatlantic cables. It is available for free download for non-commercial use from www.warriorsofthe.net and is currently available (Feb 2010) in the following languages: English, German, Spanish, Hebrew, Dutch, Swedish, French, Italian, Portuguese, Danish, Norwegian, Hungarian, and Czech. A further useful resource in order to establish the level in Internet penetration and growth in countries or regions may be found at http://www.internetworldstats.com/ It is recommended that an element of statistical information is provided within training to ensure that delegates are able to assess the impact of the Internet on their own country.

There now follows an explanation of some of the terms associated with Networks and the Internet:

- **Network Internet Card (NIC)** – is a circuit board or card installed into a computer that allows it to connect to a network
- **Media Access Control (MAC) address** – is a quasi-unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification and which provides a unique value.
- **Network Hub** - or concentrator is a device for connecting multiple twisted pair or fibre optic Ethernet devices together, making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model, and the term 'layer 1 switch' is often used interchangeably with hub. The device is thus a form of multi-port repeater. Network hubs are also responsible for forwarding a jam signal to all ports if it detects a collision.
- **Network Switch -** is a computer networking device that connects network segments. In the past, it was faster to use Layer 2 techniques to switch, when only MAC addresses could be looked up in content addressable memory (CAM). With the advent of ternary CAM (TCAM), it was equally fast to look up an IP address or a MAC address.
- **Router** - is a device that determines the next network point that a packet should be forwarded towards its destination. It must be connected to at least 2 networks. It is intelligent and works on routing tables. It is located at the gateway to a network. The term 'layer 3 switch' often is used interchangeably with router, but a switch is really a general term without a rigorous technical definition.

- **Server** – is a computer or device that provides information or services to other computers on a network. Given the right software, any network connected computer can be configured as a server. In most cases, a dedicated powerful computer designed to be "always available". One computer can run several services – e.g. web server, email server, file server, print server etc. In a business reality it often makes sense to run different services on different machines for reasons of security and to minimise the impact of any failure.
- **Local Area Network (LAN) –** is a computer network covering a small geographic area, like a home, office, or group of buildings e.g. a school. The defining characteristics of LANs, include their much higher data-transfer rates, smaller geographic range, and lack of a need for leased telecom lines.
- **Wide Area Network (WAN)** – is a computer network that covers a broad area (i.e., any network whose communications links cross metropolitan, regional, or national boundaries). Or, less formally, a network that uses routers and public communications links.
- Contrast with personal area networks (PANs), campus area networks (CANs), or metropolitan area networks (MANs) which are usually limited to a room, building, campus or specific metropolitan area (e.g., a city) respectively. The largest and most well-known example of a WAN is the INTERNET.
- **Ports** – are an endpoint or "channel" for network communications. Port numbers allow different applications on the same computer to utilize network resources without interfering with each other. Ports are 'virtual' – NOT the socket you plug into!
- **Bandwidth** – is the amount of information that can be carried through a phone line, cable line, satellite feed, and so on. The greater the bandwidth, the greater the speed of your connection and the more your Internet experience approaches a more instant-download, TV-style experience.
- **Internet Protocols** - There are quite a few of these of which the most important is the Internet Protocol (IP). Each computer connected to the Internet MUST use it. An IP Address is your Internet 'telephone number' and without an IP Addresses you would not be able to use the Internet. Different applications and services use different protocols to communicate across networks, some are: HTTP – HyperText Transfer Protocol; SMTP – Simple Mail Transfer Protocol; FTP – File Transfer Protocol; NNTP – Network News Transfer Protocol. *These are said to run "over" IP (not instead of).*[93]
- **Network Address Translation** – is a technique where the source and/or destination IP address is re-written as it passes through the firewall or router. It is most common to find it used for multiple hosts on a private network to access the Internet on a single IP address.

[93] It is recommended that any training course includes an explanation of Network addressing in some detail and in particular including: the fact that with IP version 4, addresses are in 4 groups of 3 digits (32 bit addressing) with each group numbered from 0 to 255, meaning a maximum of 256 choices. Each group called an Octet (28) and some values reserved. An explanation should be provided with details of how IP addresses are derived. This may be better achieved by a visual representation of the Binary numbering from which they are derived. Further explanation should be given of the difference between static and dynamic IP addresses and the effect this may have on investigations. An explanation of the changes in IP Version 6 should be given and the need for the change in version being that the Internet is running out of IP addresses.

3.3.3 Internet services

World Wide Web (WWW)

The World Wide Web (WWW) was effectively born in 1991 when HTML – Hyper Text Markup Language was invented by Sir Tim Berners-Lee. HTML provided the platform to combine words, pictures and sounds on web pages. Web standards are created by World Wide Web Consortium (W3C). The following explanation goes someway to explaining the name.

> "The W3 world view is of documents referring to each other by links. For its likeness to a spider's construction, this world is called the Web." *(Tim Berners-Lee, Robert Cailliau; WorldWide Web; Sept 1992*

Access to the WWW is normally achieved through the use of a Browser, which is a software program designed to locate and display web pages. The most common as of February 2010 are: Internet Explorer, Mozilla Firefox, Google Chrome, Safari and Opera.

Hyper-Text Transfer Protocol (HTTP) is the common language that Web Browsers and Web Servers use to communicate with each other on the Internet.

Though WWW browsers support a variety of protocols, e.g., FTP, NNTP, SMTP, etc., HTTP is the most frequently used protocol in combination with Web browsers. HTTP is a simple request/response (RR) protocol over TCP.

Many people mistakenly think that the WWW is in fact the Internet and this is probably because the WWW is the application used by most people. It is common for criminals to exploit that use.

In developing a training programme, consideration should be given to including examples of criminal activity on the WWW where they are relevant to the jurisdiction where the training is being delivered.

Email

Electronic Mail or Email is a method of exchanging digital messages.
To the user, It appears that E-mail is passed directly from the sender's machine to the recipient's; however each message typically passes through at least four computers during its lifetime:

1. A Message is composed on user's own computer, then sent to ISP's outgoing SMTP mail server* (Simple Mail Transfer Protocol or SMTP)
2. Outgoing ISP forwards e-mail onto recipient's ISP SMTP mail server* (SMTP – SMTP)
3. Recipient's mail server finds recipient's incoming mail server (Post Office Protocol or POP3) and delivers message to 'recipient's post box'
4. Recipient logs onto account and message is retrieved into recipient's inbox, normally deleting it from the mail server in the process

** Mail server – dedicated computer used to handle mail*

There are different types of electronic mail:

- E-mail - The traditional Outlook type mail – sent via SMTP – retrieved via POP3 and once downloaded resident on your own machine

- Web-based mail **-** POP3 mail; for instance using Outlook Express – when you log in you normally download all new mail into you inbox resident on your machine; IMAP mail – 'true' web-mail – viewed via your machine but still resident on a remote server – can be organised into folders, etc. but only visible when online.

It is often easier to compare email to a letter when explaining email. E-mail messages have a header part (the envelope), and a body part (the letter itself) with attachments. The message header is the primary focus for investigators as it contains information about sender, recipient, IP-addresses, mail servers, time-stamps etc. This information is used to assist the tracing of the sender of a message where it is not immediately apparent, for example in the case of a ransom demand issued via email. The full or extended header is vital to tracing the source of a message and it is important that Judges appreciate the difference between the headers seen when a message is delivered and the extended header that contains all the relevant information. Email is one of the most common applications that will be encountered by Judges and training designers should ensure they include the most up to date information on different types of email and how evidence about them is correctly obtained from messages themselves as well as the Internet Service Providers through who services the messages pass. Further information about email works that may be of use to training designers may be found at http://www.learnthenet.com/english/html/20how.htm

Peer to Peer (P2P)

Peer to Peer services have for many years allowed the transfer of illegal files as well as files that are subject to intellectual property rights. Peer to peer clients have been popular among criminal groups involved in these activities. First generation peer to peer architecture worked on the principle of using a centralised server to which people connected in order to download files. This made identification of those offering illegal services fairly easy to locate and close down. Second generation peer to peer clients use different methods of connectivity from those that hold lists of available files to make searching easier to those that act as supernodes that identify where files are available.

Judges will need to be aware of peer to peer activity as it may be relevant to many types of criminal and civil trial. An in depth knowledge is not necessary and training designers should consider using sites such as http://ezinearticles.com/?How-Peer-to-Peer-(P2P)-Works&id=60126 to provide up to date information.

File Transfer Protocol (FTP)

FTP is a powerful protocol that allows the transfer of files from one computer to another. It works on a client/server basis with an FTP programme installed on the client allowing the user to interact with a server in order to gain access to the services and information on the server. When a user wishes to transfer a file a TCP connection is create to the target system. User ID and password are allowed to be transmitted and the user is allowed to specify the files and the action required. When approval is given for the file transfer, another TCP connection is created for data to be transferred. Why do Judges need to know of the existence of FTP services? The answer is that they may encounter the use of such files in cases where criminals are exchanging files with each other or where FTP is used as the method of transfer by other protocols such as Internet relay Chat (IRC).

Newsgroups

The term Newsgroup is somewhat of a misleading description as they tend to host discussions. They are technically different but function in a similar way to discussion forums hosted on the World Wide Web. Newsgroup servers are hosted by various organisations who agree with others that they will synchronise their information on a regular basis. This allows users to post messages to one server and be seen by a larger audience.

Internet Relay Chat (IRC)

Internet Relay Chat (IRC) is in effect a teleconferencing system that is somewhat dated but still used by criminals to communicate and exchange files. It works by a series of servers connecting to each other and sharing messages that are posted in "Channels", which are text based, virtual meeting rooms. The discussion topics are listed and users who have an IRC client may connect to one or more channels at any time to engage in discussion with likeminded people. IRC is not the most user friendly service on the Internet and is mostly used by those who are more experienced and potentially older users. It is a protocol used by criminals and a rudimentary knowledge of its functions is required by Judges and prosecutors.

Instant Messaging (IM) and Social Networking

Instant Messaging and Social Networking have taken over as the communications tool of choice in recent years with many well known examples providing instant and user friendly access to other users throughout the world. The main feature of these sites is the ability to create a personal profile and share information about yourself and to meet new people. It is possible to share photos music and videos. The amount of personal information that is posted by individuals can make them a target for criminals for example those involved in identity theft and those wishing to groom children. Further information that may assist in the development of training materials may be found at http://communication.howstuffworks.com/how-social-networks-work.htm . Instant messaging is a form of real time direct chat between two or more individuals using shared clients. This type of chat involves contact between known person as opposed to other types of chat that allow communication between unknown persons. Criminals are known to use instant messaging as a method of communication.

3.4 How Criminals use Technology

By the end of the session participants should be able to: ➢ Explain the various ways in which technology is used by criminals.

It is important to explain at the outset that there are many terms used to describe the criminal use of technology and it may assist the reader if a brief explanation is provided. The terms "computer crime", "high-tech crime", "IT crime" and "cybercrime" are often intermingled and create confusion and misunderstanding. The use of computers and other devices by criminals and the value of recoverable data to the police investigator can be broken down as follows:

3.4.1 Technology as a victim

Technology as a target of crime – is traditionally considered to be true "computer crime" and involves such offences as hacking, denial of service attacks and the distribution of viruses.

3.4.2 Technology as an aid to crime

Technology as an aid to crime – is where computers and other devices are used to assist in the commission of traditional crimes, for example, to produce forged documents, to send death threats or blackmail demands or to create and distribute illegal material such as images of child abuse.

3.4.3 Technology as a communication tool

Technology as a communications tool – is where criminals use technology to communicate with each other in ways which reduce the chances of detection, for example by the use of encryption technology

3.4.4 Technology as a storage device

Technology as a storage medium – is the intentional or unintentional storage of information on devices used in any of the other categories and typically involves the data held on computer systems of victims, witnesses or suspects

3.4.5 Technology as a witness to crime

Technology as a witness to crime – can be found when evidence contained in IT devices can be used to support evidence to which it is not obviously related, for example to prove or disprove an alibi given by a suspect or a claim made by a witness.

3.5 Summary

This chapter has sought to provide some guidance as to the type and level of technology knowledge that is required by Judges to fulfil their role effectively. It does not purport to be a complete analysis of the issues and where relevant indicates where further information may be obtained.

It is recommended that training developers ensure that the material they prepare is as up to date and incorporates the latest technology issues as they impact on criminal behaviour; its impact on the legal, procedural and evidential rules within the jurisdiction where the training is to be delivered. There are technological changes that will affect the criminal justice system, such as solid state storage of data and Web 2.0. These will be important issues to include in training programmes and require inclusion as they become more prevalent.

As with any other programme, any training course developed for Judges should have clear objectives, which are SMART (Specific, Measurable, Achievable, Relevant and Time Bound). This is essential to be able to ensure the objectives are met. Avoid use of objectives with words such as "understand" or "know" as these do not meet the criteria. For example how do you measure if the objective of "knowing" a subject is achieved? It is better to use words such as list or identify, which are measurable. A guide to setting SMART objectives may be found at www.sheffield.ac.uk/.../Guide%20to%20setting%20objectives.doc

The use of case studies to inform the learning is considered suitable for this type of training and is more in keeping with adult learning styles than purely didactic teaching.

The key role of the training developer is to ensure the overall aim of any learning event and the specific objectives are achieved. This chapter provides some information to assist that process.

4 Cybercrime as a criminal offence

By the end of the session participants should be able to understand:

- The conduct constituting a criminal offence

It is recommended that participants have access to the text of the Convention on Cybercrime (see www.coe.int/cybercrime where the Convention can be found in different languages.

Participants should also have access to the text of their national legislation. For a number of countries, profiles are available at www.coe.int/cybercrime.

This 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.

What laws in your country cover cybercrime?

Discussion/overview of relevant domestic legislation.

4.1 Illegal access ("Hacking")

4.1.1 Phenomenon

Ever since computer networks were developed, their ability to remotely access data on another computer system has been abused for criminal purposes. The term "hacking" is used to describe the act of unlawfully accessing a computer system.[94] Due to the fact that many famous computer systems, such as those from NASA, the Pentagon, Google and the Estonian and German Government, were successfully attacked, hacking has become one of the most well known computer offences.[95] It is one of the oldest computer offences.[96] The first acts of illegal access to a computer system were discovered shortly after the introduction of network technology.[97] The offence still has great relevance in recent times.

Entering a computer system without right is very often the first act of a combination of acts, such as phishing[98] and identitiy theft.[99] The fact, that research recorded more than 250 million hacking incidents worldwide during the month of August 2007 underlines the relevance of the offence.[100]

Within the scope of recognised offences, a wide range of perpetrator's motivations has been discovered, [101] ranging 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, guarding against physical access to the computer hardware do not need to be circumvented. In addition, perpetrators do not even have to be present at the crime scene.

---

[94] 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.

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

[96] 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.

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

[98] 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.

[99] 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_co-operation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf;

[100] 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.

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

4.1.2 Legal response

Taking into account the above mentioned relevance of the offence, it might be surprising that not all countries criminalise illegal access to a computer system. One example of a country that did not criminalise illegal access to a computer system for a long time is Germany. Until 2007 such acts were intentionally not covered by the German Penal Code.[102] A prosecution was therefore only possible if the offender committed further acts such as the alteration of data.

Analysis of the various national approaches to criminalising illegal access shows a great degree of inconsistency. Some countries, such as Romania criminalise even just illegal access to a computer system[103], while others limit the criminalisation by prosecuting these offences only in cases where the accessed system is protected by security measures, or where the perpetrator has harmful intentions, or where data was obtained, modified or damaged.[104] Others do not criminalise mere access, but only subsequent offences.[105]

The Convention on Cybercrime includes a provision on illegal access that protects the integrity of the computer systems by criminalising the unauthorised access to a system. The subject of protection is of interest in maintaining the integrity of computer systems.[106]

> 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 criminalise a specific method of gaining access to a computer system. To ensure that not every development of new technology requires an amendment to the legislation, the provision was drafted by using terms that are

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

[103] 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.

[104] Opponents to the criminalisation 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.

[105] An example for this is the German Criminal Code that criminalised 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.

[106] Explanatory Report, No. 22.

neutral with regard to the technology used. The provision requires that the offender acts intentionally[107] and "without right".[108]

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.

Practical Information for judges:

Two main challenges related to illegal access are the automation of attacks and use of social engineering techniques to get access to a computer system.

As pointed out previously, surveys estimate that more than 200 million hacking attacks are carried out every month.[109] Such great numbers are the result of the availability of software tools that enable the offender to automate attacks and by this attack several hundred computer systems per day.[110] One practical challenge for judges and courts in general is the fact, that unlike the offender, they can hardly automate the necessary proceedings. This is especially relevant if the prosecution is based on incidents reported by single victims.

Another challenge appears if the offender did not use technical means, but social engineering, to get access to the computer system. Social engineering describes the manipulation of human beings – for example with the intention of gaining access to computer systems.[111] If the offender is able to manipulate the user and, for example, get his password, it is in general not sufficient to proof that he did not belong to the group of legitimate users. In this case it is – depending on the requirements regarding the consent of the victim - necessary to precisely analyse the context in which the victim disclosed the information that enabled the offender to access the computer system, in order to prove that the discloser is not legitimising the offence.

How is this offence covered under the legislation in your country?

Discussion of relevant provisions in domestic legislation and presentation of possible case studies.

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

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

[109] 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.

[110] Regarding the automation of attacks see above: Chapter 2.6.

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

4.2 Illegal interception

4.2.1 Phenomenon

During a transmission, processes in a communication network data transfer processes can be intercepted. One example of such interception is the recording of communication in a wireless network. If for example an offender succeeds in intercepting the communication between computer systems 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.[112]

4.2.2 Legal response

The Convention on Cybercrime includes a provision that protects the integrity of non-public transmission by criminalising their unauthorised interception.[113] By criminalising the illegal interception the Convention aims to equate the protection of electronic transfers with the protection of voice phone conversations against illegal tapping.[114]

> 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 criminalises 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.[115] 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.[116] 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. Similarly to the provision mentioned above, the acts must be committed intentionally and without right.

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

[113] Like Art. 2 Art. 3 enables the signatory states to adjust the extend of the criminalisation 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.

[114] Explanatory Report No. 60.

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

[116] Explanatory Report, No. 54.

Practical Information for judges:

One of the key challenges with regard illegal interception is the fact that the applicability of the provision is very much limited. As a result of the fact that the provision focuses on the criminalisation of the interception of a transfer process, that is characterised by the fact that information is transferred from the sender to the recipient, the provision is not applicable in those cases where the offender illegally obtains information stored on a computer system.[117] The access to stored information is not considered as an interception of a transmission.[118] Due to the requirement of data transfer processes, the provision is furthermore not applicable with regard to data collected by key-loggers.[119]

How is this offence covered under the legislation in your country?

Discussion of relevant provisions in domestic legislation and presentation of possible case studies.

[117] See *Gercke*, The Convention on Cybercrime, MMR 2004, Page 730.

[118] In this context not precise: Explanatory Report, No. 53.

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

4.3 Data interference

4.3.1 Phenomenon

Today more and more information is stored in a digital format, which means that the manipulation or destruction of such information can cause great damage. Unlike corporal objects, where the ability to destroy the object generally requires physical access, computer data can be in some cases be destroyed without physical access to the storage devices. One example is malicious software such as computer viruses. Computer viruses are software tools that are installed - without permission - on the victim's computer in order to carry out operations such as the deletion of data.[120]

Like illegal access, data interference can be considered a traditional computer crime. The first computer viruses had already appeared back in the 1970s. [121] Since then, not only the number of computer viruses, but also the damage they caused, has risen significantly.[122] The emerging use of networks enable the viruses to spread much more quickly than they did previously, when the exchange of disks was the main way of distribution, and infect more computer systems before the protection measures are adjusted.

One example is the "Love Bug" computer worm that was developed by a suspect in the Philippines in 2000,[123] and infected millions of computers worldwide.[124] The increasing speed of distribution influenced the damage caused by virus attacks. In 2000 the financial loss caused by malicious software was estimated to amount to some 17 billion US$.[125]

Again an example of this is the "Love Bug" computer worm developed by a suspect in the Philippines in 2000,[126] which infected millions of computers worldwide.[127] Local

[120] 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

[121] 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.

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

[123] 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.

[124] 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.

[125] *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 despite the fact, that the number of people using the Internet increased since then but the estimated losses decrease shows that the number of users of networks is only one aspect that influences the development.

[126] 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.

[127] 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.

investigations were hindered by the fact that the development and spreading of malicious software was not at that time adequately criminalised in the Philippines.[128]

4.3.2 Legal response

Article 4 of the Convention on Cybercrime includes a provision that protects the integrity of data against unauthorised interference.[129] The aim of the provision is to fill the existing gap in some national penal laws and to provide computer data and computer programs with protections similar to those enjoyed by corporeal objects against the intentional infliction of damage.[130]

> 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 does not only criminalise the damage and deletion of computer data, for example by computer virus,[131] but 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.

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

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

[130] Explanatory Report, No. 60.

[131] 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

Practical Information for judges:

One of the key challenges related to data interference is the fact that data can be deleted in a way that it is impossible to prove their existence by analysis their prior location on the hard drive.[132] In those cases, a more detailed forensic analysis of the computer system is essential to prove the act. Log files, information in a file index or system files could contain valuable evidence. This highlights the importance of close co-operation between law enforcement agencies and forensic experts and underlines the above mentioned difficulties related to the late involvement of the judges.[133]

How is this offence covered under the legislation in your country?

Discussion of relevant provisions in domestic legislation and presentation of possible case studies.

[132] Regarding the more conventional ways to delete files by using Windows XP see the Information provided by Microsoft – available at: http://www.microsoft.com/windowsxp/using/setup/learnmore/tips/waystodelete.mspx. Regarding the consequences for forensic investigations see: *Casey*, Handbook of Computer Crime Investigation, 2001; Computer Evidence Search & Seizure Manual, New Jersey Department of Law & Public Safety, Division of Criminal Justice, 2000, page 18 et. seq. – available at: http://www.state.nj.us/lps/dcj/pdfs/cmpmanfi.pdf.

[133] See above: Chapter 1.5.

4.4 System interference

4.4.1 Phenomenon

Information technology has become an important element of business communication and operation. As pointed out previously,[134] the integration of ICTs reached such a level that information societies are dependent on the availability of those services. The interruption of important services can have a negative impact on the development of the society.[135] 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 are very likely an essential part of the cybersecurity 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.[136]

Affecting the availability of services can take place in various ways. The impact of the damage of the undersea cable in 2008, which was very likely caused by anchoring ships and led to a dramatic decrease of the transmission speed in the Asian Pacific region, shows the potential of accidents.[137] But in addition to accidental interruption there are various ways that 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.[138] However, a successful attack with a computer virus requires the circumvention of protection measures. Depending on the configuration of the protection system, this can create unique difficulties, and thus a third possibility of interfering with the functioning of a computer system has become

[134] See above: Chapter 1.

[135] 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 its 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.

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

[137] Regarding the underwater cable damage see for example: US Department of Homeland Security, Daily Open Source Infrastructure Report, 4th 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, 1st February 2008 – available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9060658 ; New cable cut compounds net woes, BBC News, 4th of February 2008 – available at: http://news.bbc.co.uk/2/hi/technology/7222536.stm.

[138] 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

very popular in recent times. A number of famous web pages[139] became victim of so called "Denial-of-Service" (DoS) attacks.[140] Within such attacks the offenders are targeting a computer system with more requests than the computer system can handle.[141] Even powerful systems can be affected by these attacks.

4.4.2 Legal response

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

> 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 criminalise specific acts that lead to a system interference but covers any activity that interferes with the proper functioning of the computer system.[142] This covers physical termination of a server as well as computer virus or DoS attacks. The fact that the provision limits the criminalisation to serious attacks enables the signatory states to the Convention to limit the criminalisation to attacks against important services or cases that caused a significant damage.[143] The acts must be committed intentionally and without right.

---

[139] *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;

[140] In 2004 Internet 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.

[141] A Denial-of-Service (DoS) attack aims to make a computer system unavailable by saturating it with external communications requests, so it cannot respond to legitimate traffic. For more information, see: US-CERT, "Understanding Denial-of-Service Attacks", available at: http://www.us-cert.gov/cas/tips/ST04-015.html; *Paxson*, "An Analysis of Using Reflectors ☐for Distributed Denial-of-Service Attacks", available at: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html; *Schuba/Krsul/Kuhn/Spafford/Sundaram/Zamboni*, "Analysis of a Denial of Service Attack on TCP"; *Houle/Weaver*, "Trends in Denial of Service Attack Technology", 2001, available at: http://www.cert.org/archive/pdf/DoS_trends.pdf.In 2000 a number of well known US e-commerce businesses were targeted by denial of service attacks. A full list of the attacks business is provided by *Yurcik*, "Information Warfare Survivability: Is the Best Defense a Good Offence?", page 4, available at: http://www.projects.ncassr.org/hackback/ethics00.pdf.For more information see: *Power*, 2000 CSI/FBI Computer Crime and Security Survey, *Computer Security Journal*, Vol. 16, No. 2, 2000, page 33 et. seq; *Lemos*, Web attacks: FBI launches probe, ZDNEt News, 09.02.2000 – available at: http://news.zdnet.com/2100-9595_22-501926.html; *Goodman/Brenner*, The Emerging Consensus on Criminal Conduct in Cyberspace, page 20 – available at: http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.pdf; *Paller*, "Response, Recovery and Reducing Our Vulnerability to Cyber Attacks: Lessons Learned and Implications for the Department of Homeland Security", Statement to the United States House of Representatives Subcommittee on Cybersecurity, Science, and Research & Development Select Committee on Homeland Security, 2003, page 3 – available at: http://www.globalsecurity.org/security/library/congress/2003_h/06-25-03_cyberresponserecovery.pdf.

[142] Explanatory Report, No. 66.

[143] 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.

Practical Information for judges:

In order to increase the impact of their attack, offenders are more and more often making use of so called botnets to carry out DoS attacks. The term botnet is used to describe a group of compromised computers running programmes that are under external control.[144] If the offender uses such a botnet for a DoS attack, law enforcement agencies have to follow thousands of traces to the compromised computers first before they can evaluate if they are able to collect enough evidence to enable them to trance back the person or group controlling the botnet.

How is this offence covered under the legislation in your country?

Discussion of relevant provisions in domestic legislation and presentation of possible case studies.

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

4.5 Misuse of devices

4.5.1 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 are distributed for free, are easy to operate and can therefore even be run by users without any specific technical knowledge. The software can be used for the interception of wireless communication or the identification of open wireless networks ("Wardriving[145]"), the decryption of encrypted files or run Denial of Service (DoS)[146] 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 of a kind of black market for their production and distribution. Apart from the proliferation of "hacking devices", the exchange of passwords that enables the unauthorised user to access a computer system is taking place on a large scale.

4.5.2 Legal response

Facing this development, the drafters of the Convention decided to establish an independent criminal offence criminalising specific illegal acts regarding certain devices or access to data to be misused for the purposes of committing offences against the confidentiality, integrity and availability of computer systems or data.[147]

> 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:
> (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

[145] Wardriving is a term used to characterise 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.

[146] 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;

[147] Due to the controversial discussion on the need for criminalisation 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 criminalisation for the possession of tools and a number of illegal actions under Paragraph 1) a) – e.g. the production of such devices.

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 authorised 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 criminalisation 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 criminalising acts of preparation of crimes. In general this criminalisation – 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 criminalisation for preparatory acts to less grave offences. [148]

The connection factor of criminalisation as established by Paragraph 1 (a) is on the one hand devices[149] designed to commit cybercrimes, and on the other hand passwords that enable access to a computer system. With regard to these items, the Convention criminalised 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 harmonisation of copyrights. [150]

The Convention in general even covers devices that could be used for legal purposes if the offender intends to commit cybercrimes. Within the Explanatory Report, the drafters expressed that, in their view, the limitation to devices designed solely for the commission of crimes was considered to be too narrow, as it could lead to

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

[149] With its definition of "distributing" in the Explanatory Report ('Distribution' refers to the active act of forwarding data to others – Explanatory Report No. 72) the drafters of the Convention 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.

[150] Directive 2001/29/EC Of The European Parliament And Of The Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society:

Article 6 – Obligations as to technological measures

1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:

(a) are promoted, advertised or marketed for the purpose of circumvention of, or

(b) have only a limited commercially significant purpose or use other than to circumvent, or

(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

insurmountable difficulties of proof in criminal proceedings, rendering the provision virtually inapplicable or only applicable in rare instances.[151] To avoid too broad an application of the provision, the drafters combined a restriction on the objective level ("primarily for the purpose") and a mental element ("with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5").

Practical Information for judges:

The key challenge with regard to the misuse of devices is the proof that the interaction took place with the intent that it be used for the purpose of committing a crime. The pure possession of the devices does not indicate this intent as the software can be used for legitimate purposes as well.[152]

How is this offence covered under the legislation in your country?

Discussion of relevant provisions in domestic legislation and presentation of possible case studies.

[151] Explanatory Report, No. 73.

[152] One example for a legitimate use of such tools are security checks of websites.

4.6 Computer-related forgery

4.6.1 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" attacks.[153] 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.[154] 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") by entering his account number and password on a webpage that was set up by the offenders. The perpetrators then misuse this data.

4.6.2 Legal response

The criminalisation of the forgery of tangible items has a long legal tradition in most countries.[155] 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,

---

[153] 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.

[154] 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

[155] 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.

which require visual readability of statements or declarations embodied in a document, and which does not apply to electronically stored data.[156]

> 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.

> Practical Information for judges:
>
> As pointed out with regard to Article 6, the proof of the necessary special intent required by some provisions (such as Art. 6) very often brings unique difficulties. With regard to phishing cases the situation is slightly different. The circumstances in which the e-mails are sent out are in general a strong indication for such intent.

How is this offence covered under the legislation in your country?

Discussion of relevant provisions in domestic legislation and presentation of possible case studies.

[156] Explanatory Report, No. 81.

4.7 Computer-related fraud

4.7.1 Phenomenon

Fraud remains one of the most popular crimes in cyberspace. The success of online shopping and Internet auctions especially has increased the opportunities for offenders. The most popular crimes are credit card fraud and auction fraud.[157] Apart from these, the development of assets administered in computer systems (electronic funds, deposit money, e-gold) has become the target of manipulations similar to traditional forms of property. To avoid these criminal acts, especially with regard to Internet auctions, a number of confidence-building measures have been taken on the technical side.[158] However, the missing personal contact between the seller and customer limits the possibilities of possible victims for self-protection.

As fraud is a common problem outside the Internet as well, most national laws contain provisions criminalising 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.[159] In many cases of fraud committed on the Internet it is not a person, but a computer system, is reacting to an act of the offender. If the traditional provisions that are criminalising fraud do not integrate computer systems, an update of the national law is necessary.

4.7.2 Legal response

The Convention aims to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property by providing an article concerning computer-related fraud.[160]

> 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.

[157] "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.

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

[159] An example for 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.

[160] Explanatory Report, No. 86.

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.[161]

Under most national criminal law, the criminal act must lead to an economic loss. In addition to a general intent with regard to the elements of crime (especially the manipulation), the offence requires a special fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another. As an example, for 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 benefit to another, but are not carried out with fraudulent or dishonest intent.[162]

Practical Information for judges:

The fact that fraudulent activities involve information technology does not necessary mean that the act can be considered as an act of computer-related fraud. Very often the required differentiation between a traditional fraud committed by electronic means and a computer-related fraud that requires a manipulation of data processing is not consequently undertaken during the first phases of the investigation.

How is this offence covered under the legislation in your country?

Discussion of relevant provisions in domestic legislation and presentation of possible case studies.

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

[162] 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.

4.8 Child pornography

4.8.1 Phenomenon

In recent years the Internet has become the primary instrument for trading child pornography.[163] This development is facilitated by two main factors:

- 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. The fact that the Internet provides a global dissemination of files 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 the investigations as most of the users do not even know about the traces they leave while surfing in the Internet.[164]

4.8.2 Legal response

In order to improve the protection of children against sexual exploitation by modernising criminal law provisions, the Convention is providing an article dealing with child pornography.

> 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.

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

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

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

- The degree of a criminalisation of the mere possession of child pornography differs in the various national criminal law systems.[165] The reason for the necessity of the criminalisation of the possession of child pornography is the fact that the offenders stimulate demand for such material that could lead to ongoing production of these materials. Due to this relation between the possession and the sexual abuse of children, the drafters point out that an effective way to curtail the production of child pornography is to attach criminal consequences to the conduct of each participant in the chain from production to possession.[166] But the Convention enables the parties in Paragraph 4 to exclude the criminalisation of mere possession by restricting the criminal liability to the production, offer and distribution of child pornography.

- Article 9, paragraph 2(b) and (c) show that the legal interests covered by Paragraph 2 are wider than the direct protection of children against sexual abuse. While Paragraph 2(a) directly focuses on the protection against child abuse paragraphs 2(b) and 2(c) cover even images that were produced without violating children's rights, for example images that were completely created by use of 3D modelling software. The reason for the criminalisation of actions regarding fictive child pornography is the fact that these images could – without necessarily creating harm to a real 'child' – be used to seduce children to agree to sexual acts or to create demand for child pornography.[167]

Under its approach to improve the protection of minors against sexual exploitation the Council of Europe introduced a new Convention in 2007.[168] Already, on the first day the Convention was opened for signature, 23 states signed the Convention.[169] One of the key aims of the Convention is the harmonisation of criminal law provisions that are aiming to protect children from sexual exploitation.[170] To achieve this aim the Convention contains a set of criminal law provisions. Apart from the criminalisation of the sexual abuse of children (Art. 18) the Convention contains a provision dealing with the exchange of child pornography (Art. 20) and the solicitation of children for sexual purposes (Art. 23).

[165] Regarding the criminalisation of the possession of child pornography in Australia see: *Krone*, Does thinking make it so? Defining online child pornography possession offences Trends & Issues in Crime and Criminal Justice, No. 299; *Sieber*, Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet, is comparing various national laws regarding the criminalisation of child pornography.

[166] Explanatory Report, No. 98.

[167] Explanatory Report, No. 102.

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

[169] Austria, Belgium, Bulgaria, Croatia, Cyprus, Finland, France, Germany, Greece, Irland, Lithuania, Moldova, Netherlands, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Sweden, The former Yugoslav Republic of Macedonia, Turkey. Denmark, Iceland, Italy, Ukraine and the United Kingdom followed (July 2008).

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

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201)

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 criminalised:
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.

Article 23 – Solicitation of children for sexual purposes
Each Party shall take the necessary legislative or other measures to criminalise 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.

Article 20 of this Convention 201 is to a large degree comparable to Article 9 Convention on Cybercrime. The first main difference is the fact that the Convention on Cybercrime is focusing on the criminalisation 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, Article 20 (1) f) of the Convention on the Protection of Children criminalises the act of obtaining access to child pornography.[171] The Convention on Cybercrime does not contain such provision.

Article 23 of the Convention 201 criminalises the solicitation of children for sexual purposes by means of information and communication technology. The Convention on Cybercrime does not contain such provision.

[171] 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 – depending on the configuration of the computer system and the services used - does not involve possession of the information.

Practical Information for judges:

The offenders can make use of information technology to hide their identity while exchanging or trading child pornography pictures. In those cases, access to credit card records can be more effective than the analysis of log files.

How is this offence covered under the legislation in your country?

Discussion of relevant provisions in domestic legislation and presentation of possible case studies.

4.9 Intellectual property and related offences

4.9.1 Phenomenon

The switch from analogue to digital distribution of music and videos led to new forms of copyright violations. Millions of copyright protected songs and movies are exchanged in file-sharing systems every day.[172] Some movies even appeared in file-sharing systems before their world premiere in the cinema.[173]

The entertainment industry responded by implementing technical measures (digital rights management - DRM) to prevent the reproduction[174], 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 CDs and movie DVDs that are protected by DRM-systems. In addition, the Internet is offering the possibility to distribute the copies worldwide. As a result, the infringements of intellectual property rights, in particular of copyright, are among the most commonly committed offences on the Internet.

4.9.2 Legal response

The Convention contains a provision that is aiming to harmonise the various approaches to criminalise copyright violations in the national laws.

> 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.

[172] 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.

[173] 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.

[174] 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.

One of the main differences between Article 10 Convention on Cybercrime and most national approaches is the fact that Article 10 does not explicitly name those acts that are supposed to be criminalised, but refers to a number of international agreements – such as the WIPO Copyright treaty. This leads to criticism from those countries that are not members of WIPO.[175]

The criminalisation[176] of copyright crimes established by Article 10 Convention on Cybercrime is limited to serious cases and therefore excludes minor violations of copyrights.[177] In this context, the Convention only covers 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.

A second major limitation of the criminalisation 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.

Practical Information for judges:

The most popular versions of file-sharing systems currently enable law enforcement agencies to identify those users that are making copyright protected artwork available. This process of tracing the offenders is more difficult if the offender is using a third generation file sharing system[178] that enables anonymous communication. In those cases the trace does not necessary lead to the offender. This needs to be taken into consideration by the judge during the evaluation of evidence.

How is this offence covered under the legislation in your country?

Discussion of relevant provisions in domestic legislation and presentation of possible case studies.

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

[176] Paragraph 3 is enabling the parties to make a reservation and not criminalise copyright violations as long as they provide that other effective remedies are available and the reservation does not derogate from the parties international obligations.

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

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

5 Computer forensics and electronic evidence

By the end of the session participants should be able to understand:

- The basics of computer forensics
- The most common forensic methods
- The steps involved in securing and analysing electronic evidence.

This section contains references to more detailed information about different aspects of computer forensics and digital evidence, including the practical application of investigative techniques.

With the increasing number of cybercrimes as well as the use of ICTs in traditional offences, computer forensics and digital evidence are playing an important role in the practical work of law enforcement agencies and courts.[179] Particularly in cases where the first steps of an investigation are solely based on digital traces (as traditional evidence such as fingerprints or witnesses are not available), the ability to successfully identify and prosecute an offender is based on the correct collection and evaluation of digital evidence.[180]

[179] *Casey*, Digital Evidence and Computer Crime, 2004, page 11; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.

[180] Regarding the need for a formalisation of computer forensics see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2.

5.1 Digital evidence[181]

With the development of computer technology and its use to commit crimes, digital evidence became a new type of evidence.[182] Digital evidence is defined as any data stored or transmitted using computer technology that supports a theory of how an offence occurred.[183] Due to the shift from regular documents to computer files, digital evidence plays an important role with regard to the investigation of traditional crimes as well as cybercrime.[184]

The use of computer technology has not only introduced a new category of evidence but also influenced the way how law enforcement agencies and courts deal with evidence.[185] In the past, traditional documents were introduced in court by handing out the original document, printed on paper.

With specific regulations missing regarding the presentation of digital evidence in court, such evidence has often been presented in the form of a printout of files and other data.[186] A number of countries have started to update their legislation to enable courts to directly deal with digital evidence.[187] In spite of the transnational nature of cybercrime, the gathering of evidence is primarily governed by national regulations.

5.1.1 Challenges related to digital evidence

Digital evidence has a number of similarities to other categories of evidence. As a result, similar requirements[188] need to be taken into account when dealing with digital evidence. Law enforcement agencies need to ensure that the evidence is authentic, complete, reliable[189], accurate, and that the process of obtaining the evidence follows legal requirements.[190] At the same, a number of aspects make digital evidence unique and therefore require special attention:

- Fragile[191]. Some digital data processed by a computer system is highly fragile and can easily be deleted[192] or modified. This aspect is not only relevant for the evaluation of the digital evidence but also for the process of collecting it. Data that is solely stored in the RAM system memory will in general be lost if the system is

[181] This section takes into account contributions by Fredesvinda Insa, CYBEX.
[182] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 1; Regarding the historic development of computer forensics and digital evidence see: *Whitcomb*, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol.1, No.1.
[183] *Casey*, Digital Evidence and Computer Crime, 2004, page 12; The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: http://www.cybex.es/agis2005/elegir_idioma_pdf.htm.
[184] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol 119, page 532; *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, No.1.
[185] Regarding the difficulties of dealing with digital evidence on the basis of the traditional procedures and doctrines see: *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 57 et seq.
[186] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, p. 3.
[187] Regarding the status of national legislation see for example: The admissibility of Electronic evidence in court: fighting against high-tech crime, 2005, Cybex, available at: http://www.cybex.es/agis2005/elegir_idioma_pdf.htm; *Willinger/Wilson*, Negotiating the Minefields of Electronic Discovery, Richmond Journal of Law & Technology, 2004, Vol.X, No.5.
[188] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 19.
[189] Regarding the liability of digital investigations, see: *Casey*, Error, Uncertainty, and Loss in Digital Evidence, International Journal of Digital Evidence, 2002, Vol.1, No.2.
[190] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 161.
[191] See Casey, Digital Evidence and Computer Crime, 2004, page 16; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39.
[192] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.

shut down[193] unless special technical measures to prevent this process are applied.[194] As the information stored in the system memory can be of great importance for an investigation,[195] the technique of collecting this evidence can be different from processes of collecting traditional evidence.

- Susceptible to alteration. Digital data is susceptible to alteration. One of the most fundamental principles of computer forensics is the need to maintain the integrity of the digital evidence.[196] Ensuring a full documentation of the process and the application of methods to maintain the integrity of computer data is essential to avoid the suspect claiming that the evidence was tampered.[197] As a result, computer forensic experts seek to substitute investigation processes that lead to an alteration of files on the suspect's computer by more sophisticated processes.

- Decentralised storage. The availability of broadband access and remote storage servers has influenced the way in which information is stored. While in the past investigators were able to focus on the suspect's premise while searching for computer data, today they need to take into consideration that digital information might physically be stored abroad and only remotely accessed by the suspect if necessary.[198]

- Speed of the technical development. Technical development is continuing at a fast pace. A significant number of developments post new challenges with regard to forensic examination.[199] This development requires constant training of those who are involved in the collection of evidence, as well as keeping the forensic equipment up-to-date.[200] New versions of operating systems and other software products might generate different data that could be relevant for investigations. Similar developments take place with regard to the hardware.[201] While in the past data was stored on floppy disks, the investigators today have to take into account that relevant information might be stored in MP3 players or watches that include a USB-storage device.

[193] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.
[194] See *Haldermann/Schoen/Heninger/Clarkson/Paul/Calandrino/Feldmann/Applebaum/Felten*, Lest We Remember: Colt Boot Attacks on Encryption Keys.
[195] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 92.
[196] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1.
[197] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 162.
[198] *Casey*, Digital Evidence and Computer Crime, 2004, page 20.
[199] *Harrison/Aucsmith/Geuston/Mocas/Morrissey/Russelle*, A Lesson learned repository for Computer Forensics, International Journal of Digital Evidence, 2002, Vol. 1, No.3, page 1.
[200] Regarding the need for a formalisation of computer forensics see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2, page 2.
[201] See *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol 119, page 538.

5.1.2 Continued importance of traditional evidence

Despite the fact that during the investigation of cybercrime cases the focus will be on digital evidence,[202] other categories of evidence can play in important role in the identification of the offender as well and should therefore not be excluded. This is especially relevant because not all computer operations leave digital traces and not all existing traces can be linked to the suspect.[203] For example, if a suspect uses a public Internet café to download child pornography, it is not be possible to match the download process to an identifiable person if he did not register[204] or leave any personal information. In this case the record of a video surveillance camera could be useful if available.

With regard to those crimes that include financial transactions, the investigation should take into consideration records kept by financial organisations to identify the offender. In 2007, a global child pornography investigation was based on the identification of suspects by analysing financial transaction related to the purchase of child pornography.[205]

[202] *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 58.
[203] Regarding approaches to link a suspect to computer stored records see for example: See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 165.
[204] Regarding the obligation to register prior to the use of public Internet terminals in Italy see: *Hosse*, Italy: Obligatory Monitoring of Internet Access Points, CRi 2006, page 94.
[205] See *Schnabel,* The Mikado Principle, Datenschutz und Datensicherheit, 2006, page 426 et seq.

5.2 Computer forensics

The term computer forensics is used to describe the systematic analysis of IT equipment with the purpose of searching for digital evidence.[206] Forensics analysis usually takes place after the crime was committed.[207] Compared to regular investigations, carrying out such analysis brings unique challenges as the computer technology is constantly changing and more and more information is stored in digital formats, which increases the amount of potential evidence.[208] The focus is thereby on the ability to use the evidence in legal proceedings.[209] This limits to a certain extent the ability to carry out forensic examinations, as they are bound by the legal standards.[210] Even if new technical developments would enable new forensic investigations, their application is limited by the condition that those new instruments are covered by existing legal framework.

5.2.1 Phases of the involvement of forensic experts

Forensic experts are not only involved in criminal proceedings but also play an important role in civil proceedings, the development of protection strategies and education. With regard to criminal proceedings their involvement takes place is four phases[211]:

- Identification of the relevant evidence. Forensic experts play an important role in the design of investigation strategies. They can support the law enforcement agencies in determining the best investigation technique prior to its execution. In addition to this, consultancy forensic experts can play an active role in investigation for example by analysis of the network infrastructure in the suspect's premises, in order to identify possible locations for storage devices.[212]

- The collection and preservation of the evidence. The collection of digital evidence can take place at the physically location where they are stored as well as remotely. The investigators who are undertaking the first steps for the collection of evidence (first responder) have a significant responsibility for the entire investigation process.[213] If they make poor decisions concerning the preservation of data, important traces can be lost. One example of the challenge of the task is the issue of how to handle the running computers of the suspect.[214] Switching off the

[206] See *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 162; *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21; *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1; *Reith/Carr/Gunsch*, Examination of Digital Forensic Models, International Journal of Digital Evidence, 2002, Vol.1, No.2, page 3.

[207] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 21.

[208] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 3; *Kerr*, Searches and Seizure in a Digital World, Harvard Law Review, Vol 119, page 532.

[209] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 35.

[210] *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, Vol. 9, No. 2.

[211] Regarding the different models of Cybercrime investigations see: *Ciardhuain*, An Extended Model of Cybercrime Investigation, International Journal of Digital Evidence, 2004, Vol.3, No.1; See as well *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1 who are differentiating between six different phases.

[212] Even forensic experts will not in all cases be able to identify the storage location without the help of those people, who know the local system configuration. Regarding the ability to order people with special knowledge, such as system administrators, to support the investigation see Art. 19, paragraph 4 Convention on Cybercrime.

[213] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 88.

[214] *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 171.

electricity supply of the computer instead of shutting it down by using commands of the operating system is in general the suggested procedure. But in those cases where the offender was using encryption technology the disconnection of the electricity supply can lead to a decryption of files. Therefore the first responder needs to make a decision depending on the focus of the investigation.

Forensic expertise is not only relevant with regard to investigations taking place at the location where the relevant data is stored. Forensic experts can support an investigation as well by preparing a request that is submitted to service providers[215] and assist the investigators in producing adequate case histories[216] which are necessary to prove the reliability of the collected evidence.

- Analysis of computer technology and digital evidence. The third phase covers all aspects related to the analysis of digital evidence as well as seized hardware. It is in general the most complex phase in the whole investigation process.[217] The first responders often seize several storage devices. Each of the storage devices can contain thousands of files. The pure amount of data that needs to be analysed already brings great challenges for the investigators.[218] Identifying the relevant information for the investigation and linking it is therefore one of the major tasks of forensic experts.[219] Their work ranges from the search for illegal content in a computer system to the analysis of log-files.[220] Not all processes undertaken by the offender while committing a cybercrime leave traces. By analysing all available evidence, forensic experts can nevertheless reconstruct the way an offence was committed.[221] The third phase also includes the production of a full report which includes among other issues the steps of the investigation and the methods used to obtain evidence.

- Presentation of the evidence in court. In general forensic experts do not present the evidence in court, however they can play an important role in criminal proceedings. The forensic experts can be expert witnesses that help the people involved in the court proceedings to understand the processes of how the evidence was created, the procedures used to collect the evidence and the evaluation of the evidence.[222]

[215] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 15.
[216] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 24.
[217] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.
[218] Regarding the need for a formalisation of computer forensics see: *Leigland/Krings*, A Formalization of Digital Forensics, International Journal of Digital Evidence, 2004, Vol.3, No.2, page 2.
[219] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.
[220] For more details see below.
[221] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.
[222] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 12.

5.2.2 Examples of forensic examinations

Within the four phases (and especially within the third phase) multiple forensic examinations are possible. The choice of the right investigation technique depends on various factors – in particular, the kind of offence that is in the focus of the investigation.

Among the most common techniques are the following:

- Hardware analysis. If the investigators seize computer hardware then forensic experts can analyse the hardware to gather system-related information. Such an investigation can for example be relevant to prove whether the offender had the ability to connect a computer system to the Internet. Hardware analysis can in addition be relevant if – due to the transfer of system-related information during a registration process – it is known that the suspect used a specific hardware configuration.

- Analysis of the function of computer software. Apart from the hardware, computer software plays an important role in the operation of a computer system. Forensic experts can for example determine the functions of computer virus or other form of malicious software. In addition they can reconstruct software operation processes.[223] Furthermore, software analysis can be important to determine if the production or sale of software that can be used for legitimate as well as illegal purposes (dual-use) is criminalised.[224]

- Analysis of software installed on the suspect's computer system. An analysis of the software installed on a computer system can provide the investigators with valuable information for further investigation. This is especially the case with regard to encryption software and tools used to securely delete files.[225] If such software is installed on the suspect's computer, further investigations can specifically address those issues.

- Identification of relevant digital information. Computer data can be stored in different types of storage devices. And even within a hard disk there are various possibilities where a file can be saved. Identifying the storage location of relevant evidence is therefore challenging.[226]

  One of the new trends that presents additional challenges in identifying relevant digital information is the emerging use of remote storage. As highlighted above, the availability of broadband access and remote storage servers has influenced the way in which information is stored. By making use of such remote storage the suspect can prevent the seizure of the suspect's computer hardware enabling the law enforcement agencies to access the information that is stored on the remote storage devices. Forensic analysis can in this case be used to verify if the suspect used remote storage services.[227]

  The identification of relevant digital information is not limited to files itself. Databases of software tools used by the suspect to find information on his

[223] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 30.
[224] See above: Chapter 3.5.
[225] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9.
[226] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 24.
[227] Regarding the investigation techniques see: *Casey*, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet, 204, page 283 et seq.

computer might contain relevant information as well.[228] Even system generated temporary files might contain evidence for criminal proceedings.[229]

- Identification of hidden files. Offenders can use techniques to hide files in a storage device in order to prevent law enforcement agencies from analysing the content of the file. This is especially relevant within investigations concerning illegal content. Forensic investigations can identify hidden files and make them accessible within the analysis.[230]

- Recovery of deleted files. If the offenders are using tools to ensure that files are securely deleting, recovery of this information is in general not possible.[231] But in cases where the offenders are not aware of such tools, the deletion of digital information does not necessarily make them unavailable to law enforcement agencies as they can be recovered by using special forensic software tools.[232]

- Decrypting encrypted files and volumes and recovery of passwords**.** Criminals are more and more frequently using encryption technology.[233] This technology creates significant challenges for law enforcement agencies as they are unable to access and examine the encrypted information.[234] Within forensic analysis, approaches to decrypt encrypted files and storage devices can be undertaken.[235] In addition, forensic experts can support law enforcement agencies to develop strategies to get access to encrypted files – for example, by using a key-logger.[236]

  Offenders are able not just to prevent access to certain information by using encryption, but also use password protection systems. Forensic analysis can use

[228] *Turnbull/Blundell/Slay*, Google Desktop as a Source of Digital Evidence, International Journal of Digital Evidence, 2006, Vol. 5, No.1.
[229] *Howard*, Don't Cache out your Case: Prosecuting Child Pornography Possession Laws Based on Images located in Temporary Internet Files, Berkeley Technology Law Journal, 2004, Vol. 19, page 1227 et. seq.; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 54.
[230] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 43; *Moore*, To View or not to view: Examining the Plain View Doctrine and Digital Evidence, American Journal of Criminal Justice, Vol. 29, No. 1, 2004, page 59.
[231] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38
[232] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38.
[233] *Casey*, Practical Approaches to Recovering Encrypted Digital Evidence, International Journal of Digital Evidence, 2002, Vol. 1, No.3.
[234] *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol.10, No.3, page 473; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 38; *Gercke*, Challenges related to the Fight against Cybercrime, Multimedia und Recht, 2008, page 297.
[235] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encrpytion Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3. Regarding the decryption process within forensic investigations see: *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.
[236] *Siegfried/Siedsma/Countryman/Hosmer*, Examining the Encrpytion Threat, International Journal of Digital Evidence, 2004, Vol. 2, No.3. Regarding the forensic software magic lantern, that was developed as key-logger used by law enforcement in the US see: *Woo/So*, The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance, Harvard Journal of Law & Technology, Vol. 15, No. 2, 2002, page 521 et seq Spyware: Background and Policy issues for Congress, CRS Report for congress, 2007, RL32706, page 3; Green, FBI Magic Lantern reality check, The Register, 03.12.2001 – available at: http://www.theregister.co.uk/2001/12/03/fbi_magic_lantern_reality_check/; *Salkever*, A Dark Side to the FBI's Magic Lantern, Business Week, 27.11.2001 – available at: http://www.businessweek.com/bwdaily/dnflash/nov2001/nf20011127_5011.htm; *Sullivan*, FBI software cracks encryption wall, 2001 – available at: http://www.criminology.fsu.edu/book/FBI%20software%20cracks%20encryption%20wall.htm; Abreu, FBI confirms "Magic Lantern" project exists, 2001 – available at: http://www.si.umich.edu/~rfrost/courses/SI110/readings/Privacy/Magic_Lantern.pdf.

password recovery to enable law enforcement agencies to access password protection systems.[237]

- File analysis. Files stored on a storage device can be analysed in various ways. Forensic examinations can for example focus on the content of files. Apart from the manual examination of suspicious files, forensic investigations can include automatic keyword searches[238] for text files and tools that automatically search for known images on the suspect's computer.[239]

  As highlighted previously, computer data can be rather easily manipulated.[240] Forensic examinations can prove alterations and the forgery of digital document.[241]

  Furthermore, investigations can take into account meta-data.[242] These types of analyses can determine the time[243] the document was last opened or modified.[244] In addition, meta-data analysis can be used to identify the author of the file with a threatening message or the serial number of the camera that was use to produce child pornography image.

- Authorship analysis. If threatening texts or hate speech are posted in blogs or forums on the Internet, the analysis of log-files might not lead the investigators to the author of the text if the suspect is acting from an Internet cafe or makes use of anonymous communication services. Sophisticated linguistic analysis can help to determine if the suspect wrote articles before and left information that can help to identify the individual in this context.[245]

- Maintaining the integrity of data. As pointed out previously, the protection of the integrity of digital evidence is crucial for the admissibility in court.[246] Forensic experts can ensure the protection of the integrity of files during the collection of evidence. This enables law enforcement agencies in some cases to avoid the seizure of hardware and instead refer to copying the relevant files by protecting their integrity against any kind of alteration during the investigation process.[247] This includes in particular the creation of images of storage media.[248]

- IP tracing. Offenders that use the Internet to commit crime (for example, downloading child pornography images or attacking computer systems) leave

---

[237] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 59.
[238] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 48; *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 9; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 63.
[239] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.
[240] *Giordano*, Electronic Evidence and the Law, Information Systems Frontiers, Vol. 6, No.2, 2006, page 162.
[241] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 29.
[242] *Lange/Nimsger*, Electronic Evidence and Discovery, 2004, 6.
[243] Regarding the ability to manipulate the time information and the responde in forensic investigations see: *Gladyshev/Patel*, Formalising Event Time Bounding in Digital Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No.1; Regarding dynamic time analysis see: *Weil*, Dynmaic Time & Date Stamp Analysis, International Journal of Digital Evidence, 2002, Vol. 1, No.2.
[244] *Casey*, Digital Evidence and Computer Crime, 2004, page 16.
[245] *Chaski*, Who's at the Keyboard? Authorship Attribution in Digital Evidence Investigations, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.
[246] *Hosmer*, Proving the Integrity of Digital Evidence with Time, International Journal of Digital Evidence, 2002, Vol.1, No.1, page 1 et seq.
[247] Regarding the related procedural instrument see: Art. 19, paragraph 3 Convention on Cybercrime.
[248] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 49.

traces.[249] Traffic data analysis, such as the examination of log-files kept by Internet servers, can lead the investigators to the connection used by the offender to log on to the Internet.[250] Such investigations can be challenging if the offenders use anonymous communication technology.[251] But even in those cases investigations are not impossible. [252] One example is the forensic tool CIPAV (Computer and Internet Protocol Address Verifier) that was used in the US to identify a suspect using anonymous communication services.[253]

- E-mail analysis. E-mail has become a very popular form of communication and therefore plays an important role in computer forensics.[254] Given that it is relatively easy to identify the sender of an e-mail with threatening message or illegal content attached, offenders very often use free e-mail addresses registered using fake personal information. Even in those cases, the examination of header information[255] and log-files of the e-mail provider can in some cases enable an identification of the suspect.

- Tracing financial transactions. A number of crimes - including the sale of child pornography – include financial transaction. By using data from commercial systems and institutions involved in the financial transactions it is possible to identify the offender.[256] One example is an investigation in Germany where offenders who downloaded child pornography from a commercial website were identified by their credit card companies that analysed their customer records to identify customers that used their credit card to purchase child pornography on the specific website.[257] Such investigations are more challenging if offenders make use of anonymous payment methods.[258]

- Real time collection of traffic data and the interception of content data. Forensic investigations can include the real-time monitoring of data transfer processed. This

[249] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 57.
[250] Regarding the different sources that can be used to extract traffic data see: *Marcella/Marcella/Menendez*, Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2007, page 163 et seq.
[251] Regarding the impact on tracing offenders see: Nicoll, Concealing and Revealing Identity on the Internet in Nicoll/Prins/Dellen, Digital Anonymity and the Law, Tensions and Dimensions, 2003, page 99 et seq.
[252] *Forte*, Analyzing the Difficulties in Backtracing Onion Router Traffic, International Journal of Digital Evidence, 2002, Vol. 1, No.3.
[253] For more information about CIPAV see: *Keizer*, What we know (now) about the FBI's CIPAV spyware, Computerworld, 31.07.2007 – available at: http://www.computerworld.com.au/index.php/id;1605169326;fp;16;fpid;0; Secret Search Warrant: FBI uses CIPAV fort he first time, Heise Security News, 19.07.2007 – available at: http://www.heise-online.co.uk/security/Secret-online-search-warrant-FBI-uses-CIPAV-for-the-first-time--/news/92950; *Poulsen*, FBI's Secret Spyware Tracks Down Teed Who Teen Makes Bomb Threats, Wired, 18.07.2007 – available at: http://www.wired.com/politics/law/news/2007/07/fbi_spyware; *Leyden*, FBI sought approval to use spyware against terror suspects, The Register, 08.02.2008 – available at: http://www.theregister.co.uk/2008/02/08/fbi_spyware_ploy_app/; *McCullagh*, FBI remotely installs spyware to trace bomb threat, ZDNet, 18.07.2007 – available at: http://news.zdnet.com/2100-1009_22-6197405.html; *Popa*, FBI Fights against terrorists with computer viruses, 19.07.2007 – available at: http://news.softpedia.com/newsPDF/FBI-Fights-Against-Terrorists-With-Computer-Viruses-60417.pdf.
[254] *Gupta/Mazumdar/Rao*, Digital Forensic Analysis of E-Mails: A Trusted E-Mail Protocol, International Journal of Digital Evidence, 2004, Vol. 2, No.4.
[255] For more information see: *Crumbley/Heitger/Smith*, Forensic and Investigative Accounting, 2005, Chapter 14.12; *Caloyannides*, Privacy Protection and Computer Forensics, 2004, page 149.
[256] Casey, Digital Evidence and Computer Crime, 2004, page 19.
[257] For more information see: Spiegel Online, Fahnder ueberpruefen erstmals alle deutschen Kreditkarten, 08.01.2007, available at: http://www.spiegel.de/panorama/justiz/0,1518,457844,00.html.
[258] *Goodman*, Why the Police don't care about Computer Crime, Harvard Journal of Law & Technology, 1997, Vol.10, No.3, page 472.

enables the investigators to react to processes at the time the suspect of an investigation is acting.[259]

- Monitoring activities with regard to publicly available services. Publicly available services can be used to exchange copyright protected material or illegal content. Such services can within an investigation be monitored by forensic experts. This includes for example the observation of chat forums.[260]

- Remote forensics. Currently the need for remote forensic tools is discussed.[261] This would enable live remote evidence collection[262] and remote monitoring,[263] without the suspect being aware of investigations on his system.

Carrying out such investigations requires specific training and well defined procedures that are based on widely accepted standards and methodologies.

5.2.3 How forensic examinations are performed

There are two ways in which forensic investigations can be carried out:

- Manual operations. Despite the availability of technology to automate investigation processes, computer forensic remains up to a large degree manual work.[264] Particularly in those investigations that involve a large amount of data, such manual operations can go along with difficulties.[265]

- Analysis tools. Some of the processes – especially keyword searches, the reconstruction of deleted files or the decryption of encrypted material - can be automated by using sophisticated forensic analysis tools.[266]

Most of the investigations combine manual operations with the use of forensic software tools that automate processes.

[259] Regarding the related procedural instrument see: Art. 20 and Art. 21 of the Convention on Cybercrime.
[260] Casey, Digital Evidence and Computer Crime, 2004, page 18.
[261] Regarding the plans of German law enforcement agencies to develop a software to remotely access a suspects computer and perform search procedures see: *Blau*, Debate rages over German government spyware plan, 05.09.2007, Computerworld Security – available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9034459 ; *Broache*, Germany wants to sic spyware on terror suspects, 31.08.2007, CNet News – available at: http://www.news.com/8301-10784_3-9769886-7.html.
[262] *Kenneally*, Confluence of Digital Evidence and the Law: On the Forensic Soundness of Live-Remote Digital Evidence Collection, UCLA Journal of Law & Technology, 2005, Vol. 9, No. 2.
[263] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 52.
[264] *Ruibin/Gaertner*, Case-Relevance Information Investigation: Binding Computer Intelligence to the Current Computer Forensic Framework, International Journal of Digital Evidence, 2005, Vol. 4, No. 1.
[265] *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 62.
[266] See *Vacca*, Computer Forensics, Computer Crime Scene Investigation, 2nd Edition, 2005, page 39 et seq.; *Nolan/O'Sullivan/Branson/Waits*, First Responders Guide to Computer Forensics, 2005, page 85.; *Gordon/Hosmer/Siedsma/Rebovich*, Assessing Technology, Methods, and Information for Committing and Combating Cyber Crime, 2002, page 41 et seq.

6 Investigating cybercrime: procedural law measures

By the end of the session participants should be able to understand:

- The procedural tools that are available for law enforcement to carry out efficient investigations;
- The role of judges in this process.

It is recommended that participants have access to the text of the Convention on Cybercrime (see www.coe.int/cybercrime where the Convention can be found in different languages).

Participants should also have access to the text of their national legislation. For a number of countries, profiles are available at www.coe.int/cybercrime.

As underlined previously, cybercrime investigations carry a number of unique challenges, such as the high speed of data exchange processes or the volatility of electronic evidence. In order to react to the challenges, law enforcement need procedural instruments that enable them to take the measures that are necessary to identify offenders and collect evidence in an efficient manner.[267] Traditional investigative instruments such as search and seizure may not be sufficient. The Convention on Cybercrime therefore contains a set of special tools.

Practical Information for judges:

The Convention does not in general define the safeguards and procedural requirements for the application for each instrument. The drafter of the Convention decided not to include specific regulations in the text of the Convention, but to commit the member states to ensure that fundamental national and international standards of safeguards do apply.[268] Article 15 is based on the principle that the signatory states shall apply those conditions and safeguards that already exist under the domestic law. If the law provides central standards that apply to all investigation instruments these principles shall apply to the Internet-related instruments as well. This includes, but is not limited, to the involvement of judges in the investigation (requirement of court orders).

What provisions under your legislation apply to cybercrime investigations and the collection of evidence?

For each of the following measures, the corresponding provision in domestic procedural law should be identified and discussed, if possible, with practical examples.

[267] Regarding user-based approaches in the fight against cybercrime see: *Görling*, 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."

[268] "There are some common standards or minimum safeguards to which Parties to the Convention must adhere. These include standards or minimum safeguards arising pursuant to obligations that a Party has undertaken under applicable international human rights instruments." see: Explanatory Report to the Council of Europe Convention on Cybercrime No. 145.

6.1 Expedited preservation of data

6.1.1 The issue

The identification of a cybercrime offender often requires the analysis of traffic data.[269] In particular, the IP address used by the offender while committing the offence is an important piece of information that can help to trace back the individual. One of the main challenges to investigations is the fact that relevant traffic data are often deleted automatically within a rather short period of time.[270] 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 Article 6 EU Directive on Privacy and Electronic Communication.[271]

6.1.2 The related procedural instrument

Article 16 of the 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 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.

[269] "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.

[270] 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.

[271] 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.

This instrument should enable law enforcement agencies to react immediately after becoming aware of an offence and avoid the risk of deletion as a result of long lasting procedures.[272] After receiving such an order, the provider is obliged to preserve those data that were processed during the operation of the service.[273] Article 16 does not include an obligation on the ISP to transfer the relevant data to the authorities. The transfer obligation is regulated in Articles 17 and 18 of the Convention on Cybercrime.

In this context it is important to highlight that Article 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.[274] This would enable the authorised agencies to gain access to data that is necessary to identify an offender even month after the perpetration.[275] A data retention obligation was recently adopted by the EU Parliament[276] and is currently discussed in the US.[277]

Practical Information for judges:

The most fundamental difference between data retention and data preservation is the fact that data preservation has only a limited capability with regard to retroactive investigations, as the preservation order only forces the provider to preserve those data available at the time of the request. Data that were deleted previous to the request cannot be accessed. At the stage where judges are involved, the instrument will in general not be useful to collect evidence that was not collected during the first stages of an investigation.
As pointed out previously, states need to add safeguards and procedural requirements during the implementation process. With regard to the idea that Article 16 should enable the law enforcement agencies to immediately respond and prevent the deletion of information, a requirement of a (time consuming) court order process would be counterproductive.

[272] 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.

[273] '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.

[274] 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.

[275] 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."

[276] 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.

[277] See for example: Draft Bill to amend title 18, United States Code, to protect youth from exploitation by adults using the Internet, and for other purposes - Internet StoppingAdults Facilitating the Exploitation of Today's Youth Act (SAFETY) of 2007 – available at: http://www.govtrack.us/congress/bill.xpd?bill=h110-837. Regarding the current situation in the US see: ABA International Guide to Combating Cybercrime, page 59.

6.2 Production order

6.2.1 The issue

As mentioned above, Article 16 only obliges the provider to save those data that were processed by the provider and not deleted at the time the provider receives the order.[278] The provision does not oblige the provider to transfer the relevant data to the authorities.

6.2.2 The related procedural instrument

The transfer obligation is regulated in Article 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 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.

Article 18 of the Convention on Cybercrime is not just applicable after a preservation order was 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 apply the less intensive production order.

However the application of Article 18 is not limited to data preserved on the basis of Article 16. Article 18 can in general be applied with regard to any computer data relevant for an investigation. The ability to order the disclosure of data therefore complements the existing abilities to carry out search and seizure procedures that do not require co-operation from the person or institution that possesses the data.

Practical Information for judges:

The advantage of a separation of the obligation to preserve the data and the obligation to disclose them is the fact that it is possible to require different conditions for their application. As pointed out previously, it is recommended not to require a court order for the application of

[278] '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.

Article 16. This enables the competent authorities to react faster. The necessary protection of the rights of the suspect can be achieved by requiring a court order for the disclosure of the data.[279]

[279] The drafters of the Convention on Cybercrime tried to approach the problems related to the need for immediate action from law enforcement agencies on the one hand, and the importance of ensuring safeguards on the other in a number of ways. Another example for the approach is related to the production order (Art. 18). The drafters suggested that the requirements for the handout of data to law enforcement agencies could be adjusted in relation to the categories of data. See Explanatory Report to the Convention on Cybercrime No. 174: "The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases."

6.3 Partial disclosure of traffic data

6.3.1 The issue

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.[280]

6.3.2 The related procedural instrument

Article 18 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 law enforcement agencies 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.[281]

> Practical Information for judges:
>
> During the transmission, information in general bypasses different providers such as the Access Provider[282] and Routers.[283] Law enforcement agencies therefore need to get on a regular basis access to information that enables them to follow the path to a suspect. If the partial disclosure requires a court order, the courts should take into consideration that very often there is only a very short time frame available for such investigations. Long lasting procedures can therefore hinder such investigations.

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

[281] "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.

[282] Access Provider is a provider who is enabling users to connect to the Internet by providing dial-up or permanent Internet connection. For details see: See: *Callanan/Gercke*, Study on the Co-operation between service providers and law enforcement against cybercrime, 2008.

[283] Routers are designed to forward information from the sender to the recipient. For more details see: Khosravi/Anderson, Requirements for Separation of IP Control and Forwarding, 2003 – available at: ftp://ftp.rfc-editor.org/in-notes/rfc3654.txt.

6.4 Submission of subscriber information

6.4.1 The issue

The main aim of most cybercrime investigations is the identification of the suspects involved in committing the offences. Therefore the individualisation of the suspect is a major element 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, requires registration. The subscriber information submitted during the registration process can enable the individualisation process. This is especially the case if the submitted subscriber information is evaluated by the service provider.

6.4.2 The related procedural instrument

In addition to the obligation to submit computer data, Article 18 Convention on Cybercrime 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[284] who used the IP-address at the time of the offence. Based on Article 18 Subsection 1 b) Convention on Cybercrime, a provider is obliged to submit that subscriber information listed in Article 18 Subsection 3 Convention on Cybercrime.

[284] 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.

Practical Information for judges:

If the Internet access of a specific user or an e-mail address was used during a criminal activity, the related subscriber information can be used to identify a suspect. But it is important to point out that the subscriber information does not necessary lead to the offender. Some service providers do not for example evaluate the subscriber information submitted by the user during the registration process. If the suspect registered by using data of another person, the subscriber information will not lead to the offender. Similar difficulties can arise if the offender used an identity that he or she previously obtained illegally ("identity theft").[285]

[285] *Gercke*, Internet-related Identity Theft, 2007 – available at: http://www.coe.int/t/e/legal_affairs/legal_co-operation/combating_economic_crime/3_Technical_co-operation/CYBER/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf.

6.5 Search

6.5.1 The issue

The search and seizure is one of the most important instruments in cybercrime investigation.[286] Search and seizure of tangible objects are traditional investigation instruments in most criminal procedural codes.[287] The reason why the drafter of the Convention on Cybercrime nevertheless included a provision dealing with search and seizure is the fact that national laws do often not cover data-related search and seizure procedures.[288] Based on such provisions, the investigators would be able to seize an entire server but not seize just the relevant data by copying them.[289]

6.5.2 The related procedural instrument

> 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.
> [...]

Article 19 Subparagraph 1 of the Convention aims to establish an instrument that enables investigators to search computer systems as efficiently as they are able to perform traditional search procedures.[290] Article 19 Subparagraph 2 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 realise that the suspect did not store the relevant information

[286] 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.

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

[288] "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.

[289] This can cause difficulties in those cases where the relevant information is 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.

[290] "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.

(e.g. child pornography) on a local hard drive but on an external server that he can access via the Internet.[291] Using Internet servers to store data is becoming more and more popular.[292] 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.[293]

[291] 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

[292] 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.

[293] 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.

6.6 Seizure

6.6.1 The issue

The examination of computer systems and especially internal and external storage devices is an important aspect of computer forensics.[294] In general an investigation of the storage devices requires a physical access to the hardware. [295]

6.6.2 The related procedural instrument

> 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.

Article 19 Subparagraph 3 Convention on Cybercrime enables the law enforcement agencies to seize computer hardware.[296] In addition to the traditional seizure of the hardware, the Convention on Cybercrime enables the law enforcement agencies to copy the relevant data instead of seizing the hardware.[297] If the law enforcement agencies decide not to seize the hardware but only to copy the relevant data, there are

[294] *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;

[295] 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.

296 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.

[297] 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.

a number of side-measures provided by Article 19 Convention on Cybercrime to maintain the integrity of the copied data and remove the original data.[298]

Often the investigators will not be able to identify the exact location with the help of the system administrator that is responsible for the server infrastructure.[299] However even if they are able to identify it, the hard drive protection measures might stop them from searching for the relevant data. The drafters of the Convention therefore included an obligation on the system administrator and other people, who have knowledge about the location of stored information, to assist the law enforcement agencies.

Practical Information for judges:

Ensuring the integrity of the computer data that are necessary for the identification of a suspect or the proof of illegal activities is an essential requirement of cybercrime investigations. If the investigators do not have the permission to take the necessary measures to ensure the integrity of the copied data, these copied data may not be accepted as evidence in criminal proceedings.[300]

[298] "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.

[299] "It addresses the practical problem that it may be difficult to access and identify the data sought as evidence, given the quantity of data that can be processed and stored, the deployment of security measures, as well as the nature of computer operations. It recognises that system administrators, who have particular knowledge of the computer system, may need to be consulted concerning the technical modalities about how best the search should be conducted." Explanatory Report to the Convention on Cybercrime, No. 200.

[300] This principle applies with regard to the seizure of hardware as well. Compared to maintaining the integrity of copied data, it is often easier to maintain the integrity of data on a storage device.

6.7 Collection of traffic data

6.7.1 The issue

Traffic data play an important role in cybercrime investigation.[301] Having access to content data enables the law enforcement agencies to analyse the nature of messages of files exchanged and help to trace back 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 its physical location.

6.7.2 The related procedural instrument

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

> 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 procedures 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.[302]

[301] "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.

[302] "The article [Art. 20] does not obligate service providers to ensure that they have the technical capability to undertake collections, recordings, co-operation or assistance. It does not

Practical Information for judges:

Compared to the interception of content data[303] the collection of traffic data is in general the less intensive instrument. It does not enable direct access to the content data but to other information that can be sufficient to carry out the investigation. This aspect plays an important role in the application for a court order. Due to the existence of a less intensive instrument court might not issue an order of an interception of content data if the collection of traffic data enables the law enforcement agencies to carry out the investigation. This is especially relevant with regard to the IP-based tracing of a suspect.

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.

[303] See below: Chapter 4.8

6.8 Interception of content data

6.8.1 The issue

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 already know the communication partner and the services used, but have no information about the information exchanged. They do for example know that users who have previously been convicted for exchanging child pornography, regularly download large files from file-sharing systems, but they do not know whether these are regular – not copyright protected – movies or child pornography.

6.8.2 The related procedural instrument

Article 21 enables the law enforcement agencies to record data communication and analyse the content.[304]

> 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.

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

Practical Information for judges:

The interception of data transfer processes does not enable law enforcement agencies to analyse the content exchanged if the communication was encrypted.[305] Encryption technology can be used not only within file-exchange but also to protect voice-over-IP (VoIP) communications.[306]

[305] Regarding the impact of the se encrpytion technology on computer forensic and criminal investigations, see: See *Huebner/Bem/Bem*, "Computer Forensics – Past, Present And Future", No.6, available at: www.scm.uws.edu.au/compsci/computerforensics/ Publications/Computer_Forensics_Past_Present_Future.pdf; *Gercke*, The Challenge of fighting Cybercrime, MMR 2008, page 291 et. Seqq.

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

7 International Co-operation

By the end of the session participants should be able to understand:

- The need for widest possible and efficient international co-operation in cases related to cybercrime and electronic evidence, including urgent measures to preserve or collect data
- The international co-operation provisions of the Convention on Cybercrime.

It is recommended that participants have access to the text of the Convention on Cybercrime and its explanatory report (see www.coe.int/cybercrime where the Convention can be found in different languages).

Participants should also have access to the text of their national legislation. For a number of countries, profiles are available at www.coe.int/cybercrime.

Cybercrime has a strong transnational component[307] and attacks launched by a person in one country or jurisdiction can affect persons in multiple other countries, and even an email communication sent to a person in the same country may generate electronic evidence elsewhere as data may be transmitted through servers in several countries.

At the same time electronic evidence is volatile. Thus urgent measures that are needed to preserve data at the national level are also necessary within the framework of international co-operation.

In short, what is required is international co-operation to the widest extent possible, including urgent measures to preserve data and efficient mutual legal assistance.

Judges and prosecutors play a crucial role in such co-operation as they are either involved in approving measures or in prosecuting and adjudicating cases based on evidence obtained through international co-operation.

Chapter III of the Convention on Cybercrime provides a legal framework for international co-operation with general and specific measures. This section of the manual gives an overview of some of the provisions of this chapter.

It is essential that judges and prosecutors are familiar with these provisions but also with other existing international or bilateral agreements on co-operation in criminal matters that can be used for cybercrime cases and in particular of possibilities for direct co-operation and expedited means of communication in urgent circumstances.[308]

[307] Regarding the transnational dimension of Cybercrime see: *Keyser*, The Council of Europe Convention on Cybercrime, Journal of Transnational Law & Policy, Vol. 12, Nr. 2, page 289 – available at: http://www.law.fsu.edu/journals/transnational/vol12_2/keyser.pdf.

Sofaer/Goodman, Cyber Crime and Security – The Transnational Dimension - in Sofaer/Goodman, The Transnational Dimension of Cyber Crime and Terrorism, 2001, page 1 et. seqq. – available at: http://media.hoover.org/documents/0817999825_1.pdf;

[308] A good example is Article 4 of the 2nd Additional Protocol to the Convention on Mutual Legal Assistance in Criminal Matters (CETS 182) of the Council of Europe which provides for direct communication between judicial authorities of different countries as well as between competent authorities for mutual legal assistance or through Interpol channels. Requests can be forwarded using electronic means.

What agreements and laws can be used in your country for international cooperation in general, and in cybercrime matters in particular?

For each of the following measures, the corresponding provision in domestic procedural law should be identified and discussed, if possible, with practical examples.

7.1 General principles for international co-operation

Article 23 establishes three principles for international co-operation as provided for in Chapter III of the Convention on Cybercrime:

- international co-operation is to be provided among Parties "to the widest extent possible." This principle requires Parties to provide extensive co-operation to each other, and to minimise impediments to the smooth and rapid flow of information and evidence internationally

- co-operation is to be extended to all criminal offences related to computer systems and data as well as to the collection of evidence in electronic form related to any criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g., a murder) involves electronic evidence, the terms of Chapter III are applicable

- co-operation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international co-operation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws." The latter clause establishes the general principle that the provisions of Chapter III do not supersede the provisions of international agreements on mutual legal assistance and extradition, reciprocal arrangements as between the parties thereto (described in greater detail in the discussion of Article 27 below), or relevant provisions of domestic law pertaining to international co-operation.

The third point also explains why many European but also other countries make use of the large range of available agreements related to criminal matters when co-operating with each other against cybercrime and not exclusively the Convention on Cybercrime.

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

7.2 General principles related to extradition

Principles related to extradition are covered by Article 24 which contains a number of sub-provisions and which requires Parties to make the cybercrime offences of the Convention (articles 2-11) extraditable. At the same time it establishes thresholds so that not every offence is extraditable per se.

Article 24 also refers to other international or bilateral agreements on extradition and stipulates that in cases where an extradition is refused because of the nationality of the offender (many countries do not extradite their own nationals) the principle of "*aut dedere aut judicare*" (extradite or prosecute) applies.

Article 24 – Extradition

1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7.3 General principles related to mutual legal assistance

Article 25 repeats some of the general principles of Article 23, namely that co-operation is to be provided for to the widest extent possible and that the obligation to co-operate not only refers to cybercrimes as such but also to traditional offences involving electronic evidence.

It states that applicable mutual legal assistance treaties, laws and arrangements shall be made use of.

Parties to the Convention furthermore need to establish a national legal basis to carry out the specific measures as foreseen in articles 29 to 35 of the Convention.

Paragraph 3 of this article is aimed at accelerating the process of obtaining a response to a mutual assistance request so that critical information or evidence is not lost because it has been deleted before a request for assistance could be prepared, transmitted and responded to. It:

- empowers the Parties to make urgent requests for co-operation through expedited means of communications, rather than through traditional, much slower transmission of written, sealed documents through diplomatic pouches or mail delivery systems

- requires the requested Party to use expedited means to respond to requests in such circumstances. Each Party is required to have the ability to apply this measure if its mutual assistance treaties, laws or arrangement do not yet provide so.

Paragraph 4 sets forth the principle that mutual assistance is subject to the terms of applicable mutual assistance treaties (MLATs) and domestic laws. These regimes provide safeguards for the rights of persons located in the requested Party that may become the subject of a request for mutual assistance. For example, an intrusive measure, such as search and seizure, is not executed on behalf of a requesting Party, unless the requested Party's fundamental requirements for such measure applicable in a domestic case have been satisfied. Parties also may ensure protection of rights of persons in relation to the items seized and provided through mutual legal assistance.

Paragraph 5 is essentially a definition of dual criminality for purposes of mutual assistance under this Chapter. Where the requested Party is permitted to require dual criminality as a condition to the providing of assistance dual criminality shall be deemed present if the conduct underlying the offence for which assistance is sought is also a criminal offence under the requested Party's laws, even if its laws place the offence within a different category of offence or use different terminology in denominating the offence.

Countries that are Parties to the Convention are required to have criminalised the conduct defined in Articles 2 to 11 (illegal access, data interference, child pornography etc.) and thus the condition of dual criminality can therefore be considered as having been met.[309]

[309] Of course, some Parties may have made reservations or declarations for some of these articles reservations.

Article 25 – General principles relating to mutual assistance

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.

5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

7.4 Mutual legal assistance in the absence of applicable international agreements

The previous provisions of the Convention on international co-operation made extensive reference to the use of existing agreements. In fact, European countries dispose of a large number of such treaties as well as bilateral agreements.

However, increasingly non-European countries will become Parties to the Convention on Cybercrime and these are not necessarily acceding to other treaties on co-operation in criminal matters.

In such situations Article 27 provides the basics for mutual legal assistance between countries that have no other legal agreement.

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

7.5 Specific provision: expedited preservation of stored computer data

The expedited preservation of stored computer data is not only necessary at the national (article 16) but also at the international level. This is provided for in Article 29 of the Convention.

A Party receiving a request is obliged to act very quickly in order to have data preserved. The condition of dual criminality only applies in exceptional circumstances. It is important to underline that this is a provisional measure through which data is preserved mostly at the level of the Internet service provider. The actual disclosure of information is a subsequent step that may require a mutual legal assistance request.

Article 29 – Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

a the authority seeking the preservation;
b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
c the stored computer data to be preserved and its relationship to the offence;
d any available information identifying the custodian of the stored computer data or the location of the computer system;
e the necessity of the preservation; and
f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the

requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

7.6 Specific provision: expedited disclosure of preserved traffic data

As data often transit several countries, it is not sufficient to order the preservation of traffic data in one country but in all countries or on all servers involved in the chain. Therefore, a service provider must disclose sufficient data so that the path through which a communication was transmitted can be identified and the preservation of further data be ordered. This is provided for in Article 30 of the Convention (which is the equivalent to the partial disclosure provision under Article 17 at the national level).

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, ordre public or other essential interests.

7.7 Specific provision: mutual assistance regarding accessing of stored computer data

Article 31 allows a Party to request another Party to access, seize and disclose data stored on a computer system on its territory. This article also provides for expedited responses to requests.

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

7.8 Specific provisions: mutual assistance for the interception of data

Two provisions relate to the interception of data, namely, Article 33 which covers the real-time collection of traffic data, and Article 34 which is about the interception of content data. Of course, as the interception of content data represents a high level of intrusion, mutual assistance in this respect is restricted and subject to safeguards, other applicable treaties and domestic law.

Article 33 – Mutual assistance in the real-time collection of traffic data

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

7.9 Specific provision: the network of 24/7 points of contact

In order to facilitate urgent action, in particular the expedited preservation of data in another country, a network of 24/7 points of contact has been established under Article 35 of the Convention.[310] Each Party is required to establish a point of contact for co-operation in urgent cases. This point of contact supplements and does not replace other existing channels of co-operation.

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;
b the preservation of data pursuant to Articles 29 and 30;
c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

[310] This provision is based on the experience of the G8 High-tech Crime Subgroup which established such a network already in 1997.

8 Appendix

8.1 Case examples

CHAPTER 3.1 – ILLEGAL ACCESS: THE KGB HACK

Back in the year 1986, when the network system nowadays referred to as the Internet connected mostly computers run by the scientific community and the military, a group of German computing enthusiasts from the area of Hanover discovered a security flaw concerning a small program called *movemail*, which allowed them to gain rights for reading and writing files on a remote machine and thus access to its file system. By utilizing the software vulnerability and exploiting existing network topologies, the group around *Karl Koch, Markus Hess* and *Dirk Breschinski* managed to connect to and explore many computer systems around the world, some of them owned and operated by the University of California in Berkeley, the NASA and even the Pentagon.

In an effort to turn their expertise into profits, the German hacker group tried to take advantage of cold war tensions and contacted the Soviet secret service KGB in East Berlin in order to sell sensitive information and secrets found on U.S. computer systems. After some debate, an agreement had been reached, which required the hackers to deliver examples of their work. In the following months, mostly military information has been exchanged for several ten thousand West German Marks.

In 1987, the hackers' cover was blown by *Clifford Stoll*, who then worked as a system administrator at the Lawrence Berkeley National Laboratory. Hunting down 0.75 Cents worth of computing time that could not be charged to a user's account, *Stoll* found out that someone had illegally accessed the computer system he was accountable for. *Stoll* worked with U.S. and German authorities to track down the perpetrators, which finally were located by tracing back data packets to the telephone connection of *Markus Hess*.

Hess and *Breschinski* were prosecuted and received a probation sentence for violating substantive criminal code that had been put into force just in time to cover their deeds as spies for the Soviet Union in 1986. *Koch* was guaranteed exemption from punishment in return for the details he provided, but presumably committed suicide as a consequence of drug abuse and mental disorders even before his collaborators were put on trial. The whole KGB hack case attracted worldwide attention and has been recognized as one of the first international computer crime incidents that demonstrated just how vulnerable networked systems and the data stored within actually are – and how unimportant geographical distances might actually be in the information age.

CHAPTER 3.2 – ILLEGAL INTERCEPTION: THE TJX DATA THEFT

The U.S. retail giant TJX, parent company to popular American outlets TJ Maxx, Marshalls and Office Maxx, and its customers became the victims of what is considered one of the largest data theft operations ever discovered: Between 2005 and 2007, nearly 100 million credit card numbers had been stolen by means of illegal interception. The hacker group around *Albert Gonzalez* also managed to capture some personal customer data and operated on the company's network unnoticed for at least seven months.

At the heart of the hackers' operation stood a sniffing device – a computer running software that listens to data streams being transported over a network. The intruders discovered that TJX was transferring credit card numbers along with other customer and checkout related data to their financial service companies over wireless networks. Moreover, the credit card numbers were secured by a weak and outdated encryption standard. To benefit from these security loopholes, the group around *Gonzalez* planted sniffer software on computers owned and operated by TJX. The sniffers listened to the wireless network and grabbed the data by copying it on the fly.

During and after the raid, the credit card numbers were sold through underground trade forums to so-called "carders", who produce fake credit cards and withdraw cash at automatic telling machines. By selling the stolen data, the TJX hackers allegedly obtained more than a million dollars. They have been identified and indicted in 2008; while three hackers turned out to be U.S. citizens, the group consisted also of three Ukrainian and two Chinese hackers, as well as members from Belarus and Estonia. In the summer of 2009, *Gonzalez*, who is considered to be the head of the group, agreed to a guilty plea that might lead to a sentence of 15 to 25 years in prison.

It has been estimated that the incident might cost TJX up to 1.7 billion dollars in compensation for damages. The data theft also gave reason to the Payment Card Industry Security Standards Council to release guidelines and standards U.S. companies have to obey when dealing with credit card transaction data.

CHAPTER 3.3 – DATA INTERFERENCE: THE LOVE BUG WORM

Just when the digital world had stepped into the 21st century without being affected by the feared and predicted Year-2000-trouble, a malicious piece of software spread across the globe in mere hours and caused severe computer trouble nobody had expected at all. The Love Bug worm – also called Loveletter worm or "I-Love-You-Virus" despite its classification – was created and turned loose in the Philippines. From its first appearance on May 4, 2000 it took only one day to affect computers connected to the Internet on a worldwide scale.

The worm itself consisted of a visual basic script, i.e. a small piece of computer code that exploited security flaws in Microsoft's Windows operating system. The worm concealed its true nature posing as a love letter attachment to an e-mail message and thus tricked users into clicking and launching the attachment. Once activated, the Love Bug worm propagated itself by sending identical e-mail messages to all recipients found in the address book of the infected computer, which explains the fast spread of the worm. Furthermore, it deleted multimedia files such as MP3 songs and JPG pictures and left a copy of itself with the name of the deleted file instead. By generating an unexpected high volume of network traffic, the Love Bug worm also caused mail servers and other systems to crash repeatedly, thus leaving their functions and stored data temporarily unavailable.

The impact of the Love Bug worm was unprecedented: Nearly ten percent of all computers connected to the Internet were affected, forcing press companies to deliver heavily thinned emergency issues of newspapers and taking down mail servers of governments, parliaments and international companies alike. It has been estimated but not confirmed that the total damage due to unavailable data caused by the Love Bug worm piled up to more than 5.5 billion dollars.

Malware experts were quickly able to trace the outbreak back to the Philippines and – with the help of the FBI, local authorities and Internet providers – finally identified the people responsible for creating and disseminating the Love Bug worm. But while a search warrant had been carried out in due time, it was not possible to prosecute the incident and bring the culprits to court: In the year 2000, the Philippine criminal code lacked any provision to penalize the deed described above.

CHAPTER 3.4 – SYSTEM INTERFERENCE: THE LUFTHANSA BLOCKADE

Virtual "sit-in" demonstration or criminal system interference? That question rose in Germany in 2001, when a human rights group called to take a stand against the German airline Lufthansa, which also serves as air carrier for deportations of aliens without permit to stay. The people behind the group "Libertad!" opposed the act of deportation and the role of Lufthansa concerning deportations; they chose the day of Lufthansa's annual shareholder meeting to show their express criticism on the whole matter by blocking the website of the airline from functioning.

In order to do so, the "Libertad!" people distributed flyers pointing to their website and their cause. From their website, anyone could download a software which was programmed to repeatedly and automatically access the website lufthansa.com at a specified time. More than 13.000 people responded to the call and either used the software or accessed lufthansa.com manually, which resulted in a distributed denial-of-service attack: Although warned and prepared with additional capacities, the Lufthansa web server could not handle the amount of requests and shut down. Therefore, the computer system Lufthansa customers rely on for booking flights and looking up flight information was unavailable or only partially available for up to two hours.

The people from "Libertad!" registered their protest project as demonstration with German administrative authorities, but Lufthansa did not share the political view of their "protest" and filed a criminal complaint against the owner of the "Libertad!" domain. In 2005, the local district court convicted the defendant of coercion and instigating others to commit criminal actions. In 2006, however, a regional appeal court acquitted the defendant. Both verdicts met a lot of criticism: While the local district court failed to consider § 303a/b StGB, the German substantive criminal code provisions that correspond to Article 5 of the Convention on Cybercrime, the regional appeal court interpreted the element of data suppression in such a manner, that temporary suppressions would not suffice for a conviction. Subsequently, critics warned that denial-of-service attacks on websites were not punishable if the opinion of the appeal court became accepted.

CHAPTER 3.5 – MISUSE OF DEVICES: SELF-DENUNCIATIONS IN GERMANY

Germany sports a vivid IT security scene with a long tradition of so-called "white hat" hacking, i.e. probing systems and software to show security flaws that need to be fixed in the best interest of vendors and users. That is why a fierce discussion developed over the measure of adopting Article 6 of the Convention on Cybercrime as § 202c StGB within the German substantive criminal code. It was the dual-use difficulty that spurred the resistance of institutions like the Chaos Computer Club and many IT security professionals.

A dual-use tool is typically software that IT security professionals and white-hat hackers rely on to behave like an attacker or intruder, which is very often the only way to efficiently check if security measures work as intended. While the Convention of Cybercrime speaks of devices, including computer programs, which are designed *primarily* for the purpose of committing offences, the German § 202c StGB penalizes the preparation of offences by offering, obtaining etc. software *whose purpose* is *to commit* such an offence. The critics found fault with the fact that this provision does not expressly exclude the use of such tools for security reasons, leaving the risk of prosecution to any individual IT security professional and thus having a negative impact on the industry as a whole.

As soon as the amendment had passed and went into force, the IT security magazine iX's editor in chief, *Jürgen Seeger*, and an entrepreneur in the IT business, *Herbert Treinen*, denunciated themselves, asking law enforcement authorities to prosecute them in order to create legal certainty, whether working in their job was now illegal. However, their criminal complaints against themselves were turned down with respect to the lack of wilful intent. Another criminal complaint had been filed against the *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, the German governments IT security office. The BSI offered a set of tools that could be download from its homepage which contained "Jack the Ripper", a password cracking tool that had been wildly popular a while ago. Just as before, the complaint was turned down due to the lack of wilful intent to prepare an offence.

Finally, the German constitutional court rejected several constitutional complaints against § 202c StGB in 2009; since the rejection resulted from formal legal requirements, the court did not have to deal with substantive arguments – and, unfortunately, did not provide any legal guidelines for the term *purpose*.

CHAPTER 3.6 – COMPUTER-RELATED FORGERY: PHISHING

The sum of criminal acts commonly known as phishing should rather be understood as phenomenon than being exemplified by a single case. This is due to the degree of industrialization the phishing business has developed recently: From the first sightings of manually performed phishing schemes in 2003 and 2004, the attacks have grown more and more professional over the years, with software kits like *Rock Phish* being available. *Rock Phish* works mostly automated and allows non-technophile people to launch phishing scams without the need of knowledge about deep details of the process; if needed, the vendors even offer support via IRC chat sessions. Investigations in the U.S. and in European countries show that phishing is still on the rise, which can be blamed to some extent on the fact that nowadays phishing is not a technical challenge any more.

Although largely automated, the process of phishing consists in great parts inevitably of acts of forgery: In the beginning, e-mail messages will be created with the purpose to convince the recipients of their authenticity, pretending to originate from the recipients bank and asking to click on a link that in turn pretends to lead to some security check. At the same time, a website has to be maintained at a domain that leaves the victim unsuspicious. In order to do so, officially looking bank logos are used and original bank websites are imitated in a way close to perfection. There are, however, other phishing scams employing trojan horses, i.e. malware, instead of e-mails and websites. Such malware typically hooks up to the communication between the victim's computer and the bank's web server, altering the data stream on the fly; in that case, other articles of the Convention on Cybercrime would apply.

CHAPTER 3.7 – COMPUTER-RELATED FRAUD: PREMIUM RATE DIALER

Premium rate dialers had become very popular in the late 1990s, as they allowed providers of premium content on the Internet to charge their offers separately on the phone bill, thus eliminating the need to put in sensitive credit card data on websites. Usually dialers are implemented as small computer programs or scripts, which add a network connection that dials a premium rate number. However, dialers were soon discredited: Fraudsters utilized the fact that dialer software can be programmed to clandestinely change the default connection settings to a premium rate number. The dialer therefore manipulated the victims' system, resulting in massive phone bills. With the rise of broadband connections such as DSL, the number of cases involving premium rate dialers has decreased.

With respect to auction-related fraud on sites like eBay, on the contrary, computer-related fraud is usually not applicable: While an Internet connection, the auction platform's website and the input of information on the auction itself might be used to facilitate criminal activities, the falsity of the victim as a natural person is still an indispensable element leading to the fatal bid. Therefore, auction-related fraud is fully covered by traditional fraud provisions.

CHAPTER 3.8 – CHILD PORNOGRAPHY: OPERATION MARCY

Due to the pressure on commercial child pornography websites enforced by cyber-cops policing and patrolling the web – since the late 1990s, such special branches have been deployed by many countries –, the consumers of child pornography had to think about other ways of seeking and distributing their criminal assets. That is the main finding of "Operation Marcy", a comprehensive investigation against child pornography on the Internet, which was started in 2002 and brought up more than 25.000 suspects in 166 countries, consequently attracting much attention in the media when the preliminary results were published in the fall of 2003.

Operation Marcy began with a hint towards a web forum that contained child pornographic pictures. Looking into the matter, the police discovered bit-by-bit 38 private circles with members from all over the world, where incriminated material had been exchanged. The suspects used web forums protected by user/password combinations, allowing access and membership only after new users had qualified. In order to do so, new members had to show some of the child pornography material they already possessed to prove their loyalty. Some of the suspects used the web forums only to contact other consumers, and then met in person to exchange their respective images and videos offline.

The success of Operation Marcy was largely facilitated by the cooperation of an international provider who worked closely with the police, handing over 26.500 image files, 38.000 sets of e-mail address data and 12 gigabyte of log files with more than 14 million entries documenting individual access events. The investigation was named after the prime suspect, whose first name is Marcel – the revealing of his activities in the web forum he founded was the first domino piece that led to an unprecedented number of suspects in cybercrime investigations.

CHAPTER 3.9 – INTELLECTUAL PROPERTY: FTPWELT.COM

Digitalisation and broadband data connections have facilitated lossless copying and fast transfers of almost any kind of content by a great deal. But while it is still fiercely discussed to what extent the favourite teenage pastime of downloading music through file sharing systems actually hurts the media industry, another group of people took the exploitation of songs, movies, games and software through digital means to a new level: By offering vast amounts of pirated music, the latest Hollywood blockbusters and so-called warez in exchange for monthly fees or single payments, criminals take advantage of the same fundamental technological revolution as the previously mentioned youth.

FTPWelt.com used to be such a pirate and warez trafficking spot. The operators of the site had close ties with so-called release groups, who compete among each other for releasing cracked software or movies even before they are available in stores and cinemas; the latter is often achieved by bribing projectionists and other cinema staff. FTPWelt.com offered all types of cracked software and media files on extremely reliable and fast FTP servers rented in the Netherlands, the U.S. and Russia to ensure high performance service for their customers. At peak times, the site made profits of about 120.000 euro per month with more than 45.000 customers.

In 2004, however, investigations of the computer magazine *c't*, the Berlin-based newspaper *Tagesspiegel* and the society for the prosecution of copyright infringement (*GVU*) led to search and seizure operations concerning the operators and a Munich-based attorney responsible for the handling of payments and other administrative tasks. As business masquerade, the gang had created a company called "Internet Payment Systems Ltd." based in Tortola, British Virgin Islands. All persons involved have been indicted under a legal provision that corresponds to Article 10 of the Convention on Cybercrime and in 2007 were finally sentenced to imprisonment terms up to 23 months on probation and fines of up to 90.000 euro due to guilty pleas. The FTPWelt.com case is considered to be one of the biggest successful operations against copyright infringement on a commercial scale.

CHAPTER 5.1 AND 5.3 – EXPEDITED DATA PRESERVATION AND PARTIAL DISCLOSURE OF TRAFFIC DATA: BOTNET CLIENTS AS PROXY SERVERS

IP addresses are the common denominator of every crime committed online: The inconspicuous line of numbers reveals the perpetrator at best, will at least provide further leads and will be logged to any kind of network process on the Internet – in the majority of cases, it even proves to be the only lead available. But in a steeply rising number of investigations, the IP address used by the offender is intentionally pointed towards an unsuspicious third party; thus, ordering the preservation of data for the victim's or its provider's systems might turn out to be insufficient.

A good example of such case facts is the phenomenon of botnet clients that are used as proxy servers. A botnet consists of several hundred, sometimes tens of thousands of malware-infected computers and is controlled by a criminal, the botmaster. The infected computers within the rogue network are mostly owned privately and function properly, so everything seems to be in order for their unsuspicious owners. In fact, however, the botmaster commands the infected clients and rents their service out to paying customers. Renting a botnet client as proxy server is quite common and provides some degree of anonymity: By making a connection through the infected botnet client, an offender assumes the IP address and thereby the identity of the infected computer.

In these scenarios, the partial disclosure of traffic data that originated from the third party's infected computer might prove to be helpful: Since communication works usually bi-directional, on request of the offender some data packets should have been sent back to him. Unfortunately, the chain of proxies used by an offender can be quite long – due to the ephemeral nature of traffic data, the challenge is to puzzle out the chain links before there is no data left to be preserved by order.

CHAPTER 5.2 AND 5.4 – PRODUCTION ORDER AND SUBMISSION OF SUBSCRIBER INFORMATION: SPREAD OF RELEVANT DATA

Within only a decade, executive authorities all over the world had to adopt to important paradigm shifts they had not expected: Before the 1990s, telecommunication operators in most countries used to be state-run or publicly controlled agencies. At that time, nobody thought about problems associated with the access to subscriber information in order to support a criminal prosecution connected to a call or telegram: After all, some public authority already had the relevant data available, and accessing it was just a question of administrative assistance. After privatizing most of their telecommunication services, however, many states had to legally ensure future access to that data, which then not only fell into the hands of private companies, but also soon became subject to extensive data protection regulations.

At the same time, the rise of the Internet and its popular services like e-mail, chat and others led to a huge broadening of possibilities and techniques to communicate with one another on a global scale. Therefore, new players such as e-mail providers joined the ranks of gatekeepers with respect to subscriber information. In the early gold rush years of the world wide web, especially smaller service and content providers often proved to be reluctant to cooperate with law enforcement authorities – an expression of distrust quite common within parts of the IT community at that time. Therefore, as subscriber information can clearly be of great help in individualizing suspects, victims and other persons linked to an investigation, the necessity of production order provisions was out of the question.

Nowadays, the spread of relevant data – not only confined to subscriber information – has become almost unmanageable: The so-called web 2.0 technology helped create social networks where millions of people exchange messages, photos and other data, as well as blogs and micro blog services like Twitter. Furthermore, any Internet user can found his or her own forum – password protected accounts with subscriber information included – for free. Thus, in the web 2.0 era, it's even more important to ensure proper access, if needed, to stored computer data and first and foremost to subscriber information – even if it's kept on record by amateur forum administrators.

CHAPTERS 5.5 AND 5.6 – SEARCH AND SEIZURE: PERSONAL DATA STORED ON THE EMPLOYER'S HARDWARE

Traditionally, evidence used in criminal investigations comes in some kind of tangible format – be it a weapon, a tissue sample or a fingerprint. Therefore it's only natural when provisions dealing with the search for and seizure of evidence are closely connected to its physical and spatial conditions. With respect to electronic evidence, however, these requirements might seem partly inappropriate or even obstructive, depending on the legal positions at stake: While prosecutors searching for intangible information sometimes help themselves by simply seizing all of the hardware that belongs to a suspect, the suspect or a third party might have objections to such a measure as being disproportional or even be barred from certain defense positions.

A good example of the latter is a case dealt with by the German constitutional court in 2007: The suspect worked as a public servant and used an office computer, which was owned by his employer, among other things, to send and receive both private and work-related e-mails. The investigating law enforcement authorities had reason to believe that the suspect received and forwarded an e-mail with a power point presentation containing incriminated material. The computer was handed over to the authorities and checked for digital evidence. The suspect objected to this measure, appealing to the local court to check the legitimacy of the seizure. However, his appeal was rejected both by the local court and the higher district court: The suspect had no legal standing to challenge the measure, because the computer did not belong to him.

The German constitutional court upheld these decisions and rejected the complaint filed by the suspect, since the criminal courts made no mistake in applying the relevant legal provisions that could have infringed the suspect's fundamental constitutional rights. While that decision is correct in a formal way, the applied legal provisions themselves clearly show that intangible evidence could not be handled properly and thus led to the loss of a formal defense position: After all, the data in question could be allocated to the suspect; the sought-after "piece" of digital evidence had without a doubt been created by him. Therefore, it would be perfectly reasonable to grant him a formal defense position to challenge measures with respect to "his" data.

CHAPTER 5.7 – COLLECTION OF TRAFFIC DATA: EXTORTION VIA E-MAIL

When criminals try to conceal their online moves, the analysis of traffic data can be very helpful. In the year 2009, a criminal who considered himself to be clever attempted to extort a large sum from a retail chain with stores in various European countries. The man threatened to poison certain products of a store brand promoted by the retail chain. All of his threats and claims were sent via e-mail. However, the clever criminal used different e-mail accounts registered with different providers, which could only produce the falsified data the suspect had filled into the registration forms. Even worse, the IP address data logged to each e-mail delivery pointed to various access providers in different countries, including China and the U.S.

Upon thorough examination, the IP address data retrieved from the e-mail headers could be linked to a proxy service offering anonymization by downloading and utilizing a certain program. Since the operator of such an anonymization service is generally able to individualize a user's connections, a real-time collection of traffic data has been ordered with the following provision: Traffic data should only be collected for the individual who attempts to connect with the suspect's known e-mail accounts through the anonymization service. The idea proved successful: The real-time collection of traffic data revealed the true IP address of the suspect, which in turn led to a name and an address that advanced the investigation.

CHAPTER 5.8 – INTERCEPTION OF CONTENT DATA: INVESTIGATIONS INTO ORGANIZED CYBER CRIME

While the concept of lawful interception has long been known for telephone calls, lawmakers around the world obviously couldn't have had the new communication methods available over the Internet's IP technology in mind. However, besides more or less important technical issues, there is no big difference between the various forms to exchange information, be it over a phone line, in a chat room or by downloading a document from a server: the content might just be the same.

As more and more people start to shift their communication habits from classic calls to textual information sent over the Internet, it's natural in a quite obvious sense when law enforcement authorities' interest in these communication channels equally grows. But recent investigations have shown that organized groups of cyber criminals – people who offer background services like connectivity for malware and phishing sites as well as notorious data thieves – have embraced communication via IP technology long ago and hardly communicate any other way. For example, some suspects in the enormous TJX data theft case (see page 4, chapter 3.2) were only identified and/or convicted by means of intercepted chat messages. According to federal police agents familiar with such cases, listening to IRC channels is also a well-proven method for structural investigations within a network of loosely connected cyber criminals.

8.2 Glossary of terms

ADDRESS

The term address is used in several ways.
- An Internet address or IP address is a unique computer (host) location on the Internet.
- A Web page address is expressed as the defining directory path to the file on a particular server.
- A Web page address is also called a Uniform Resource Locator, or URL.
- An e-mail address is the location of an e-mail user (expressed by the user's e-mail name followed by an "at" sign (@) followed by the user's server domain name.

ADVANCE FEE FRAUD

A scam based on the promise of revenue after the victim has transferred a fee in advance.

ADWARE

Software that periodically displays advertisements on the user's computer.

ARCHIVE FILE

A file that contains other files (usually compressed files). It is used to store files that are not used often or files that may be downloaded from a file library by Internet users.

AMERICAN STANDARD CODE FOR INFORMATION INTERCHANGE (ASCII)

A coding standard for interchanging information expressed mainly by the written form of English words. ASCII is implemented as a character-encoding scheme based on the ordering of the English alphabet, and is used to represent text in computers, communications equipment, and other devices that work with text. Formerly the most commonly-used character encoding on the World Wide Web, ASCII was surpassed in 2008 by UTF-8.

AUTHENTICATION/AUTHENTICITY

Authentication is the security goal of being able to prove or verify a person's or entity's identity with a certain level of assurance. Authentication mechanisms are used to provide access control to information systems.

Authenticity is the security goal of being able to prove or verify that an electronic message or transaction originated from a particular person or source with a certain level of assurance.

BACKDOORS[311]

A backdoor is malicious code that allows unauthorised access to a computer system or network by accepting remote commands from at attacker elsewhere on the Internet. Backdoors allow attackers to execute remote commands and install other software, which may in turn compromise passwords or other personal data, or allow the machine

[311] OECD Malware study

to be used for further nefarious purposes. Remote access or backdoor functionality is typically now included in most trojan and bot programmes. A bot programme is a type of 'backdoor' programme that allows attackers to remotely control many compromised information systems (often thousands) simultaneously (or individually). Backdoors intentionally but ill-advisedly included in legitimate software products to facilitate remote customer support become exploitable vulnerabilities when discovered by malicious actors.

BACKUP

A copy taken of all information held on a computer in case something goes wrong with the original copy.

BIOS

Basic input output system. A programme stored on the motherboard that controls the basic startup operations for the machine. Bios searches for the processor, memory, IDE (Integrated Drive Electronics) devices, and ports. Bios completes POST (Power On Self Test) checks and compares results with CMOS. BIOS executes Config.sys and Autoexec.bat which are stored on the root directory (for dos OS this is C:>)

BLUETOOTH

Bluetooth is a telecommunications industry standard which allows mobile phones, computers and personal digital assistants (PDAs) to connect using a short range wireless connection.

BOOKMARKING

The process of storing the address of a website or internet document on your computer, so that you can find it again easily.

BOOT

To start a computer, more frequently used as "re-boot".

BOOT DISK

Refers to a floppy disk that contains the files needed to start an operating system

BOT

A computer that has been infected with a piece of malware and is now controlled by a miscreant, to be used for their own purposes without the knowledge or consent of its owner. Often used to launch DDoS attacks, send spam, act as a proxy server, and spread malware to additional systems. Usually connects to some type of C&C mechanism to receive additional instructions, updated malware, etc. This C&C may be HTTP- or IRC-based, or may consist of a harder-to-track P2P network. A bot may be infected with multiple pieces of malware and connected to multiple C&Cs simultaneously, under the control of more than one miscreant.

BOTNET

A group of bots running the same or similar malware, connecting to the same C&C mechanism. Botnets can range in size from a handful of individual bots to thousands,

even millions of bots. Their effectiveness depends on the type of malware they are infected with, as well as the type of hosts infected – a small number of hosts on large bandwidth Internet links (such as computers at corporations or universities) may have more destructive power than a large number of hosts on highly restricted links.

BUFFER

An area of memory, often referred to as a "cache", used to speed up access to devices. It is used for temporary storage of the data read from or waiting to be sent to a device such as a hard disk, CD-ROM, printer or tape drive.

BULLETIN BOARD SERVICE (BBS)

A BBS is like an electronic corkboard. It is a computer system equipped for network access that serves as an information and message-passing centre for remote users. BBSs are generally focused on special interests, such as science fiction, movies, Windows software, or Macintosh systems. Some are free, some are fee-based access, and some are a combination.

BYTE (binary term)

In most computer systems, a byte is a unit of data generally consisting of 8 bits. A byte can represent a single character, such as a letter, a digit, or a punctuation mark.

CACHE

A cache (pronounced CASH) is a place to store something more or less temporarily. Web pages you browse to are stored in your browser's cache directory on your hard disk. When you return to a page you've recently browsed to, the browser can get it from the cache rather than the original server, saving you time and the network the burden of some additional traffic. Two common types of cache are cache memory and a disk cache.

CDF

Channel Data Format, a system used to prepare information for Webcasting.

CD-R

Compact disk – recordable. A disk to which data can be written but not erased.

CD-ROM (COMPACT DISC READ-ONLY MEMORY OR MEDIA)

In computers, CD-ROM technology is a format and system for recording, storing, and retrieving electronic information on a compact disk that is read using laser optics rather than magnetic means.

CD-RW

Compact disk – rewritable. A disk to which data can be written and erased.

CHAT ROOM

Available through online services and some electronic bulletin boards. Allows the real-time exchange of messages between users of a particular system.

CIRCUIT BOARD

A thin plate with chips, devices and other electronic components installed on the plate.

CLICK FRAUD

A type of crime that occurs when a person, automated script, or computer program pretends to be a legitimate user by clicking on an online advertisement, for the purpose of generating revenue or increasing costs to an advertiser in a pay-per-click advertising setting.

CMOS – COMPLEMENTARY METAL-OXIDE SEMI-CONDUCTANT.

This is a low power memory chip that holds basic functionally data such as the power on password, time & date, drive search sequence and hard drive types. This is often confused with the BIOS chip. Basically the BIOS chip gets the computer up and running and COMPARES what it finds against the settings saved the last time in the CMOS.

COMMAND AND CONTROL SERVER (C&C)

A Command & Control server (commonly "C&C") is the point of control for a piece of malware. It may not be a single server, as malware uses a variety of connection mechanisms that can include IRC, HTTP, and P2P, and may include multiple, sometimes rapidly changing, servers.

COMPUTER DATA

Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function[312]

COMPUTER SYSTEM[313]

Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

CPU (CENTRAL PROCESSING UNIT)

The most powerful chip in the computer. Located inside a computer, it is the "brain" that performs all arithmetic, logic and control functions.

CRACKER

A computer expert that uses his or her skill to break into computer programmes or DVDs protected by key encryption systems. Usually these are proprietary items under copyright. The Cracker will then make the 'Cracked' software or DVD available for free or at reduced costs.

[312] Article 1 of the Convention on Cybercrime
[313] Article 1 of the Convention on Cybercrime

CRYPTOGRAPHY

Cryptography is most often associated with scrambling **plaintext** (ordinary text, sometimes referred to as cleartext) into **ciphertext** (a process called **encryption**), then back again (known as **decryption**). Individuals who practice this field are known as cryptographers. The process of securing private information that is sent through public networks by encrypting it in a way that makes it unreadable to anyone except the person or persons holding the mathematical key/knowledge to decrypt the information.

DATABASE

Structured collection of data that can be accessed in many ways. Common database programs are: Dbase, Paradox, Access. Uses: various including – address links, invoicing information, etc.

DELETED FILES

If a subject knows there are incriminating files on the computer, he or she may delete them in an effort to eliminate evidence. Many computer users think that this actually eliminates the information. However, depending on how the files are deleted, in many instances a forensic examiner is able to recover all or part of the original data.

DENIAL OF SERVICE ATTACKS (DOS)

Denial of Service Attacks are aimed at specific Web sites. The attacker floods the Webserver with messages endlessly repeated. This ties up the system and denies access to legitimate users.

DIGITAL SIGNATURE

A code which is used to guarantee that an e-mail was sent by a particular sender.

DIGITAL VIDEO (DV)

Video captured, manipulated and stored in a digital format.

DISK CACHE

A portion of memory set aside for temporarily holding information read from a disk.

DISC SPACE

Disc storage. The space on the web hosting a company's server/computers that a web site's content is allowed to utilise.

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

A denial of service attack carried out by a large number of distinct systems, usually compromised systems infected with bots and part of a botnet. The large number of sources can make identification of legitimate traffic vs. attack traffic difficult, and can hinder mitigation efforts.

DOMAIN NAME

A Domain Name is the identifier or address of any entity on the Internet.

DOMAIN NAME REGISTRANT (REGISTRANT)

An individual or company that has registered a domain name through a domain name registrar. The registrant is generally considered the legal owner or administrator of a domain name.

DOMAIN NAME REGISTRAR (REGISTRAR)

A company that has been accredited by the appropriate authority to register Internet domain names. These companies provide domain name registration services to end users, and can be looked at as the "retailer" in the domain registration business model, and are usually (but not always) distinct from the domain name registry.

DOMAIN NAME REGISTRY (REGISTRY)

A database of all domain names registered within a particular top-level domain. Also used to refer to the registry operator, the organization which manages this database, controls the policies for registration of names, and produces the zone files for the top-level domain. The registry can be looked at as the "wholesaler" in the domain registration business model.

DOMAIN NAME SYSTEM (DNS)

The system that provides the mapping from an Internet domain or host name, such as www.team-cymru.org, to a resource address or identifier – often this is the IP address of the server that provides service for that domain or host name, such as 68.22.187.6. A DNS record may also map to a nameserver that is authoritative for a domain or subdomain, or a mail server that is configured to process mail for that domain or subdomain.

DONGLE

A term for external hardware devices with some memory inside it. Companies that sell expensive software packages use dongles as proof that a computer actually has a licence for the software being used. It would be built in for the software to search for the dongle connection prior to allowing itself to.

DVD

Digital versatile disk. Similar in appearance to a compact disk, but can store larger amounts of data.

ENCRYPTION

The process of scrambling, or encoding, information in an effort to guarantee that only the intended recipient can read the information.

E-MAIL HEADER

E-mails come in two parts – the body and the header. Normal header information gives the recipient details of time, date, sender and subject. All e-mails also come with extended headers – information that is added by e-mail programs and

transmitting devices – which shows more information about the sender that is in many circumstances traceable to an individual computer on the Internet.

EXPANSION BOARD

A printed circuit board that can be inserted into a computer to add capabilities.

FILE TRANSFER PROTOCOL (FTP)

A network protocol used to exchange and manipulate files over a network. FTP operates in clear-text, and does not provide strong security. SFTP is a secure variation on FTP that runs over an SSH connection and provides end-to-end encryption.

FILTERING

Internet filtering systems prevent or block users' access to unsuitable material.

FIREWALL

A network security system used to restrict external and internal traffic.

GIGABYTE (GB)

1 Gigabyte = 1024 Megabytes. A gigabyte is a measure of memory capacity and is roughly one thousand megabytes or a billion bytes. It is pronounced GIG-a-bite with hard G's.

HACKER

Persons who are experts with computer systems and software and enjoy pushing the limits of software or hardware. To the public and the media, they can be good or bad. Some hackers come up with good ideas this way and share their ideas with others to make computing more efficient.
However, some hackers intentionally access personal information about other people with their expertise, and use it to commit computer crimes. See Cracker.

HARD DISC

The hard disk is usually inside the PC. It stores information in the same way as floppy disks but can hold far more of it.

HARDWARE

The physical parts of a computer. If it can be picked up it is hardware as opposed to software.

HOST MACHINE

For the purpose of this document a host machine is one which is used to accept a target hard drive for the purpose of forensically processing.

HYPERTEXT TRANSFER PROTOCOL (HTTP)

The protocol used by web browsers to request and receive web pages from servers on the Internet.

INSTANT MESSAGE (IM)

A broad term for a form of real-time communication between two or more people based on typed text, conveyed via devices connected over a network such as the Internet. Some common IM networks and protocols include AOL Instant Messenger (AIM), ICQ, Yahoo IM, MSN Messenger, Jabber, and Google Talk. IRC is sometimes considered an instant messaging medium, though it traditionally falls into a slightly different category.

INTERNET PROTOCOL (IP)[314]

The Internet protocol is the native language of programmatic communication on the Internet. The Internet Protocol allows large, geographically diverse networks of information systems to communicate with each other quickly and economically over a variety of physical links. An IP address is the numerical address by which an Internet-connected computer is identified. Information systems on the Internet use IP addresses to route traffic and establish connections among themselves.

INTERNET PROTOCOL ADDRESS (IP ADDRESS)

The numeric address assigned to a computer on the Internet, something like 192.0.2.42 in IPv4 or 2001:db8:a8bc::4853 in IPv6.

IRC - INTERNET RELAY CHAT

A virtual meeting place where people from all over the world can meet and talk about a diversity of human interests, ideas, and issues. Participants are able to take part in group discussions on one of the many thousands of IRC channels, or just talk in private to family or friends, wherever they are in the world.

ISP – INTERNET SERVICE PROVIDER

A company that sells access to the Internet via telephone or cable line to your home or office. This will normally be by free - where the user pays for the telephone charge of a local call - or by subscription - where a set monthly fee is paid and the calls are either free or at a minimal cost. See also "Service Provider.

KEYLOGGER/*LEYSTROKE LOGGERS*[315]

A keystroke logger is a hidden programme that records and "logs" each key that's pressed on the compromised system's keyboard, as the legitimate user of the system is typing, in the process recording personal data like usernames, passwords, credit-card and bank account numbers. Keystroke loggers secretly store the data away in hidden files that is eventually transmitted to a remote collection point, elsewhere across the network. Keystroke logging functionality is typically included in most trojan programmes.

KILOBYTE (KB)

1 Kilobyte = 1024 bytes.

[314] OECD Malware study
[315] OECD Malware study

LINUX

An operating system initially designed to provide users with a free alternative to Unix and Microsoft. Because of its many free distribution versions this OS is now used in a wide range of commercial products and is typically seen in servers and network architecture rather than at user level. Linux and Unix based OS's represent over 50% of the internet architecture. Linux is a favoured tool of experienced hackers as it allows them to control to a very high degree all interaction from their machine to the victim machine. It also allows them to circumvent 'security' measures in DOS based systems with relative ease.

MACRO VIRUS

A virus attached to instructions (called macros) which are executed automatically when a document is opened.

MAGNETIC MEDIA

A disk, tape, cartridge, diskette, or cassette that is used to store data magnetically.

MALWARE

Malicious software designed to infiltrate or damage a computer system without the owner's consent.

MEGABYTE (MB)

1 Megabyte = 1024 Kilobytes.

MEMORY

Often used as a shorter synonym for random access memory (RAM). Memory is the electronic holding place for instructions and data that a computer's microprocessor can reach quickly. RAM is located on one or more microchips installed in a computer.

MONITOR

What the PC displays the information on.

MOUSE

Device that, when moved, relays speed and direction to the computer, usually moving a desktop pointer on the screen.

OPERATING SYSTEM

This software is usually loaded into the computer memory upon switching the machine on and is a prerequisite for the operation of any other software.

ORB

A high capacity removable hard disk system. ORB drives use magnetoresistive (MR) read/ write head technology.

PACKET[316]

A packet is the minimum autonomously-routable quantum of data which can be transmitted across a modern digital "packet switched network." It consists of a "header" of routing, addressing, and protocol information, followed by a "payload" of data. A packet is a message containing data as well as the destination address that is transmitted over a network that transmits packets, or "packet switching networks."

PAYLOAD

A payload is the essential data that is being carried within a packet or other transmission unit. The payload does not include the "overhead" data required to get the packet to its destination. Note that what constitutes the payload may depend on the point-of-view. To a communications layer that needs some of the overhead data to do its job, the payload is sometimes considered to include the part of the overhead data that this layer handles. However, in more general usage, the payload is the bits that get delivered to the end user at the destination.[317]

PASSWORD

A word, phrase, or combination of keystrokes used as a security measure to limit access to computers or software.

PCMCIA CARDS

Similar in size to credit cards, but thicker. These cards are inserted into slots in a Laptop or Palmtop computer and provide many functions not normally available to the machine (modems, adapters, hard disks, etc).

PERSONAL COMPUTER (PC)

A term commonly used to describe IBM & Compatible computers. The term can describe any computer useable by one person at a time.

PERSONAL ORGANISER OR PERSONAL DIGITAL ASSISTANT (PDA)

These are pocket-sized machines usually holding phone and address lists, and diaries. They often also contain other information.

PHISHING

Phishing ("Fishing for Passwords") is a term used to describe the action of assuming the identity of a legitimate organisation, or web site, using forged email and/or fraudulent web sites and with a view to convince consumers to share their personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. for the purpose of using it to commit fraud. This is often referred to as Identity Theft.

PIRATE SOFTWARE

Software that has been illegally copied.

PORT

[316] OECD Malware study
[317] OECD Malware study

The word port has 3 meanings.

Where information goes into or out of a computer, e.g. the serial port on a personal computer is where a modem would be connected.

On the Internet Port often refers to a number that is part of an URL appearing after a colon (:) right after the domain name. This is a virtual gateway in or out of the computer in the same way as the physical ports described above. Ports allow specific programmes to connect over the Internet between machines. EG all basic http web traffic operates on port 80. All standard email operates on port 110.

It also refers to translating a piece of software to bring it from one type of computer system to another, e.g. to translate a window programme so that it will run on a Macintosh. (PORTING).

PRETTY GOOD PRIVACY (PGP)

A computer program that provides cryptographic privacy and authentication. PGP is often used for signing, encrypting, and decrypting e-mails to increase the security of e-mail communications. An OpenPGP standard was defined in RFC 4880 to allow for interoperability of applications implementing PGP.

PROXY SERVER

A server on the Internet that acts as a go-between for requests from clients seeking resources from other servers. May be used to work around access restrictions on the client's Internet connection, and/or to hide the client's identity. Systems infected with malware are often configured to act as proxy servers so that the controllers of the botnet can use them or sell their services (for sending spam, breaking into web sites, etc).

PUBLIC DOMAIN SOFTWARE

Programmes that are 'free'. Also known as freeware.

QUERY

To search or ask. In particular to request information in a search engine, index directory, or database.

RAM

Random access memory is the PC's short-term memory. It provides working space for the PC to work with data. Information stored in the RAM is lost when the PC is turned off.

REMOVABLE MEDIA

Items e.g. floppy disks, CDs, DVDs, cartridges, tape that store data and can be easily removed.

REMOVABLE MEDIA CARDS

Small-sized data storage media which are more commonly found in other digital devices such as cameras, PDA's (Personal Digital Assistants) and music players. They can also be used for the storage of normal data files, which can be accessed and written to by computers.

The cards are non-volatile – they retain their data when power to their device is stopped – and they can be exchanged between devices

ROOTKIT[318]

A rootkit is a set of programmes designed to conceal the compromise of a computer at the most privileged "root" level, by modifying operating system files or inserting code into the memory of running processes. As with most malware, rootkits require administrative access to run effectively, and once installed can be virtually impossible to detect. The role of the rootkit is simply to conceal evidence of the compromise to the user, the operating system and other applications (e.g., anti-virus or anti-spyware products) designed to detect the presence of the malicious files that have been installed on the computer. In most cases, once a rootkit is installed anti-virus and anti-spyware products will not work. However, a rootkit is not required to effectively conceal the presence of the malware. Many types of malware disable, or have mechanisms for bypassing security counter-measures installed on a computer without using a rootkit.

SERVICE PROVIDER[319]

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

SHAREWARE

Software that is distributed free on a trial basis with the understanding that if it is used beyond the trial period, the user will pay. Some shareware versions are programmed with a built-in expiration date.

SMARTCARD

Plastic cards, typically with an electronic chip embedded, that contain electronic value tokens. Such value is disposable at both physical retail outlets and on-line shopping locations.

SOCIAL ENGINEERING

This refers to techniques designed to fool human beings into providing information or taking an action which leads to the subsequent breach in information systems security. Examples of social engineering include telephoning the IT help desk and pretending to be an employee when and asking for your password to be reset in order to gain unauthorised access to an employee's computer account and the network; or sending an email impersonating a victim's bank in order to get the victim to click on a phishing URL and provide their bank account password into the fake attacker-controlled web site. Social engineering is the computer industry's term for what are more generally referred to as "confidence scams." The term is intended to make a distinction from

[318] OECD Malware study
[319] Article 1 of the Convention on Cybercrime

computer engineering or software engineering, in that social engineering uniquely attacks the human component of an information system.

SOFTWARE

The pre-written programs designed to assist in the performance of a specific task, such as network management, web development, file management, word processing, accounting or inventory management.

SPAM

Spam is commonly understood to mean bulk, unsolicited, unwanted and potentially harmful electronic messages. There appears to be a growing correlation between malware and spam. It is important to note that only a discussion of Spam that is used as a vector for the distribution of malware is within the scope of this report.[320]

SPOOFING

The creation and sending of IP packets with a forged (spoofed) source IP address. This may be done to conceal the identity of the sender or impersonate another computer system, or it may be used to create a "backscatter" effect, with responses to the spoofed traffic going to a victim host that was used as the fake source IP.

SPYWARE[321]

Spyware is a form of malware that is capable of capturing a range of data from user input (keyboards, mice) and output (screens) and other storage (memory, hard drive etc) and sending this information to the attacker without the user's permission or knowledge. Some spyware tracks the websites a user visits and then sends this information to an advertising agency while malicious variants attempt to intercept passwords or credit card numbers as a user enters them into a web form or other applications.

SYSTEM UNIT

Usually the largest part of a PC, the system unit is a box that contains the major components. It has the drives at the front and the ports for connecting the keyboard, mouse, printer and other devices at the back.

TAPE

A long strip of magnetic coated plastic. Usually held in cartridges (looking similar to video, audio or camcorder tapes), but can also be held on spools (like reel to reel audio tape). Used to record computer data, usually a backup of the information on the computer.

TRAFFIC DATA

Any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service[322]

[320] OECD Malware study
[321] OECD Malware study
[322] Article 1 of the Convention on Cybercrime

TROJAN (HORSE)[323]

A Trojan horse is a computer programme that appears legitimate but actually has hidden functionality used to circumvent security measures and carry out attacks. A trojan horse may enter a user's computer by presenting itself as a compellingly attractive tool of some sort, which the user intentionally downloads and installs, unaware of its ulterior purpose. Trojans typically build in the functionality of keyloggers and other spyware and a range of other functions to disable system security.

UNIX

A very popular operating system. Used mainly on larger, multi-user systems. Unix based systems control the majority of primary functions on the internet and represent over 50% of the internet web servers in use today.

USB STORAGE DEVICES

Small storage devices accessed using a computer's USB ports, that allow the storage of large volumes of data files and which can be easily removed, transported – and concealed. They are about the size of a car key or highlighter pen, and can even be worn around the neck on a lanyard.

VIDEO BACKER

A program, that allows computer data to be backed up to standard video. When viewed the data is presented as a series of dots and dashes.

VIDEO CONFERENCING

A live connection between people in separate locations for the purpose of communication, usually involving audio and often text as well as video.

VIRUS[324]

Directly analogous to its biological namesake, a virus is hidden code that spreads by infecting another programme and inserting a copy of itself into that programme. A virus requires its host programme to run before the virus can become active and generally requires human interaction to activate. Viruses deliver a payload which could contain a simple message or image thus consuming storage space and memory, and degrading the overall performance of your computer, or in the case of a more malicious payload, destroy files, format your hard drive, or cause other damage. Viruses were the very earliest form of malware, appearing first in the 1970s as escaped experiments from academic computer science labs and experimental teenagers, and most of the early ones would be better characterized as the effects of bad judgment than ill intent.

WEBCAM

A webcam is a camera connected to the internet. A live picture, or snapshot, is uploaded to a website from the camera at regular intervals, typically every few

[323] OECD Malware study
[324] OECD Malware study

minutes. By looking at the web page from which the camera operates, you can see what the camera sees – almost as it happens.

WEBLOG

A weblog, commonly know as a blog, is a form of online diary or journal. They contain short, frequently updated posts, arranged chronologically with the most recently posted item appearing at the top of the page. In addition to text, blogs can contain photos, images, sound, archives and related links, and can incorporate comments from visitors.

WORD PROCESSOR

Used for typing letters, reports and documents. Common Word Processing programs: Wordstar, Wordperfect, MS-Word.

WORM[325]

A worm is a type of malware that self replicates without the need for a host programme or human interaction. Worms generally exploit weaknesses in a computer's operating system or other installed software and spread rapidly from computer to computer across a network and/or the Internet. Worms and viruses are the only types of malware that can self-propagate. Increasingly, the terms 'virus' and 'worm' are used interchangeably.

WIRELESS NETWORK CARD

An expansion card present in a computer that allows cordless connection between that computer and other devices on a computer network. This replaces the traditional network cables. The card communicates by radio signals to other devices present on the network.

ZIP DRIVE/DISK

A 3.5-inch removable disk drive. The drive is bundled with software that can catalogue disks and lock files for security.

[325] OECD Malware study