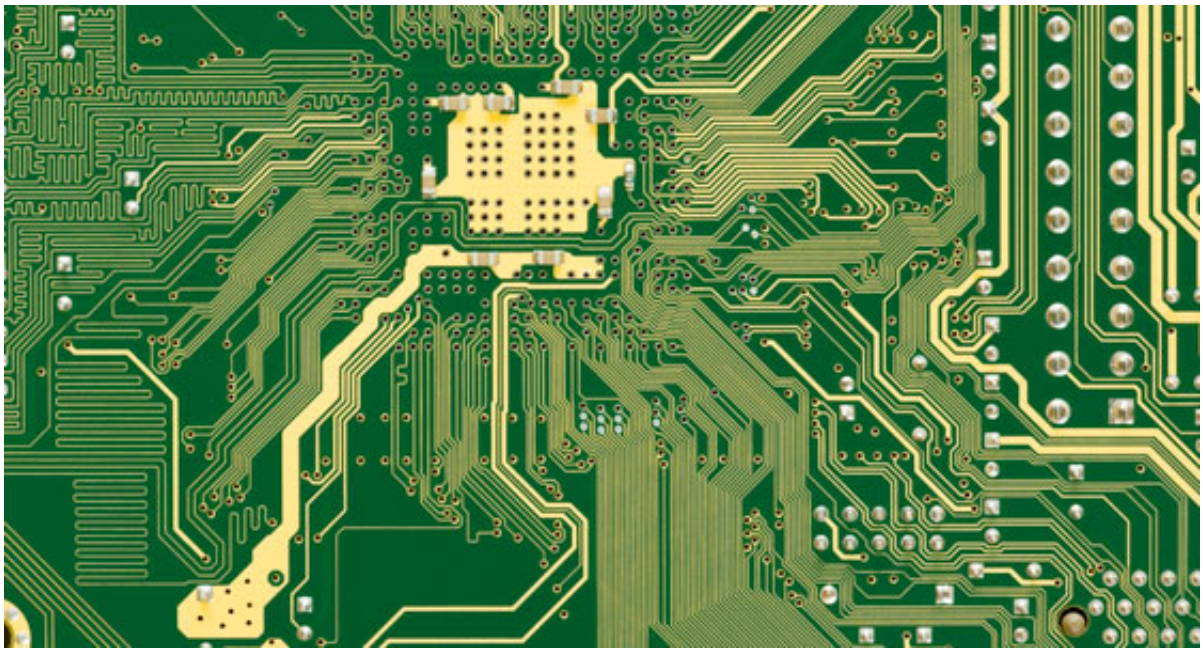
FROM ENCRYPTION TO FAILURE OF TRADITIONAL INVESTIGATION INSTRUMENTS

The shift from industrial societies to information societies,(1) and the related dependence of the society as well as the economy on the availability of Internet services have moved the attention of politics towards the cybercrime topic.

While in other emerging areas of crime it is possible to use traditional crime prevention and investigation strategies, the fight against cybercrime faces unique challenges that require a special attention from both investigators and lawmakers. This article provides an overview of some of those challenges.



1. Availability of tools and instructions to commit Cybercrime

In the early days of computer crimes, committing an offence required a significant amount of technical understanding. Nowadays however, offenders can commit cybercrimes by using software devices that do not require in-depth technical knowledge, such as software tools (2) designed to locate open ports or break password protection.(3) Due to mirroring techniques and peer-to-peer exchange, it is difficult to limit the widespread availability of such devices (4) that can potentially turn any computer user into a cybercriminal. Furthermore, offenders can use the Internet to find instructions on how to commit crime, both online and offline. For example, the term “Googlehacking” (or “Googledorks”) describes the use of complex search engine queries to filter many search results for information on computer security issues.(5) Several reports emphasised the risk of the use of search engines for illegal purposes.(6) An offender planning an attack can find detailed information on the Internet explaining how to build a bomb by using only chemicals that are available in regular supermarkets.(7)
2. Resources

Offenders can use sophisticated methods to increase their resources. An example of this is represented by botnet attacks such as those used in 2007 against computer systems in Estonia.(8) An analysis of the attacks

suggests that they were committed by thousands of computers within a “botnet,”(9) a group of compromised computers running programs under external control. Over recent years, botnets have become a serious risk for cybersecurity.(11) The size of a botnet can vary, from a few computers to more than a million computers.(12)

3. Difficulties in tracing offenders

Although users leave multiple traces while using Internet services, offenders can hinder investigations, and in particular their identification, by resorting to special services. For example, if they use public Internet terminals that do not require identification, investigations will often falter. Offenders can also make use of open wireless networks to hide their identity. While difficulties in identifying Internet users have the potential to support democratic processes, they also go along with fears of abuse perpetrated by offenders.

4. Failure of traditional investigation instruments

An effective fight against terrorist use of the Internet requires Internet-specific tools that enable competent authorities to carry out investigations.(13) In a growing number of Internet-related cases, traditional investigation instruments are not sufficient to indentify an offender. One example is the interception of Voice-over-IP (VoIP) communication.(14) In the last decades, States have developed investigation instruments (such as wiretapping) that enable them to intercept landline as well a mobile phone communication.(15) The interception of traditional phone calls is usually carried out through telecom providers.(16) Applying the same principle to VoIP, law enforcement agencies would operate through ISPs and service providers supplying VoIP services. However, if the service is based on peer-to-peer technology, service providers may generally be unable to intercept communications, as the relevant data are transferred directly between the communicating partners.(17) Therefore, new techniques, as well as the related legal instruments, might be needed.

5. Missing control instruments

The Internet was originally designed as a military network(18) based on a decentralised network architecture that sought to preserve the main functionality intact and in power, even when individual components of the network were attacked. Carrying out investigations in this environment goes along with challenges, as the designer of the network did not include control instruments.(19)

Recent trends to implement technology blocking access to websites(20) are an approach to compensate the absence of control instruments. Norway,(21) Sweden,(22) Switzerland,(23) the United Kingdom,(24) Italy,(25) China,(26) Iran(27) and Thailand(28) are among those countries that require or encourage blocking access to illegal contents stored outside the country. While this in general seems like an example of the possibility of introducing control instruments, the ability of users to circumvent filter technology(29) using encrypted anonymous communication services shows the limitation of such approach.

6. Transnational nature of the offence

The Internet is a good example of globalisation, with services generally available to all Internet users. As a consequence, many data transfer processes affect more than one country.(30) If offenders and targets are located in different countries, cybercrime investigations require the cooperation of law enforcement agencies in all the countries affected,(31) as national sovereignty does not permit investigations within different States territories without the permission of local authorities.(32) The related formal requirements and time needed to collaborate with foreign law enforcement agencies often hinder investigations,(33) which often occur in very short timeframes. Offenders may deliberately include third countries in their attacks to make investigation more difficult.(34)

7. Independence of location and presence at the crime site

One constituting fact common to all types of cybercrimes is the fact that offenders do not need to be present at the same location as the victim. Offenders can therefore act from locations where there is either no effective legislation in place or it is not enforced.(35) Preventing such “safe havens” has therefore become a key intention of international approaches in the fight against cybercrime.(36)

8. Encryption technology

Another challenge is the use of encryption technology by offenders.(37) Encryption is a classic example of a

neutral technology, since as it is not only used to hinder investigations but also to prevent unauthorised access to information. It is therefore considered a key technical solution for ensuring cybersecurity.(38) The latest operating systems offer the possibility to encrypt computer data with the click of a mouse, making it difficult for law enforcement agencies to break the encryption and access the data.(39) It is uncertain to what extent offenders already use encryption technology to mask their activities, but it has been reported, for instance, that terrorists are already using encryption technology.(40)

* Dr. Marco Gercke is the Director of the Cybercrime Research Institute.

1 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.

2 “Websense Security Trends Report 2004”, page 11; Information Security - Computer Controls over Key Treasury Internet Payment System, GAO 2003, page 3; Sieber, Council of Europe Organised Crime Report 2004, page 143.

3 Ealy, “A New Evolution in Hack Attacks: A General Overview of Types, Methods, Tools, and Prevention”, page 9.

4 In order to limit the availability of such tools, some countries criminalise the production and offer of such tools. An example of such a provision can be found in Art. 6 of the European Convention on Cybercrime.

5 For more information, see: Long/Skoudis/van Eijkelenborg, “Google Hacking for Penetration Testers, 2005”; Dornfest/Bausch/Calishain, “Google Hacks: Tips & Tools for Finding and Using the World’s Information”, 2006.

6 See Nogguchi, “Search engines lift cover of privacy”, The Washington Post, 09.02.2004.

7 One example is the “Terrorist Handbook” – a pdf-document that contains detailed information how to build explosives, rockets and other weapons.

8 Regarding the attacks, see: Lewis, “Cyber Attacks Explained”, 2007, “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.

9 See: Toth, “Estonia under cyber attack”, http://www.cert.hu/dmdocuments/Estonia_attack2.pdf

10 See: Ianelli/Hackworth, “Botnets as a Vehicle for Online Crime”, 2005, page 3.

11 See “Emerging Cybersecurity Issues Threaten Federal Information Systems”, GAO, 2005, available at: http://www.gao.gov/new.items/d05231.pdf

12 Keizer, Duch “Botnet Suspects Ran 1.5 Million Machines”, TechWeb, 21.10.2005.

13 This was as well highlighted by the drafters of the Council of Europe Convention on Cybercrime that contains a set of essential investigation instruments. The drafters of the report point out: “Not only must substantive criminal law keep abreast of these new abuses, but so must criminal procedural law and investigative techniques“ see: Explanatory Report to the Council of Europe Convention on Cybercrime No. 132. Regarding the substantive criminal law provisions related to Cybercrime see above: Chapter 6.1.

14 The term “Voice over Internet Protocol” (VoIP) is use to describe the transmission technology for delivering voice communication by using packet-switched networks and related protocols. For more information see: Swale, Voice Over IP: Systems and Solutions, 2001; Black, “Voice Over IP”, 2001.

15 Regarding the importance of interception and the technical solutions see: Karpagavinayagam/State/Festor, "Monitoring Architecture for Lawful Interception in VoIP Networks, in Second International Conference on Internet Monitoring and Protection" – ICIMP 2007; Regarding the challenges related to interception of data communication see: SwaleChochliouros/Spiliopoulou/Chochliouros, "Meassures for Ensuring Data Protection and Citizen Privacy Against the Threat of Crime and Terrorism – The European Response", in Janczewski/Colarik, "Cyber Warfare and Cyber Terrorism", 2007, page 424.

16 Regarding the differences between PSTN and VoIP communication see: Seedorf, "Lawful Interception in P2P-Based VoIP System"s, in Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 et seq.

17 Regarding the interception of VoIP by law enforcement agencies, see Bellovin and others, "Security Implications of Applying the Communications Assistance to Law Enforcement Act to Voice over IP"; Simon/Slay, "Voice over IP: Forensic Computing Implications", 2006; Seedorf, "Lawful Interception in P2P-Based VoIP Systems", in Schulzrinne/State/Niccolini, Principles, Systems and Applications of IP Telecommunication. Services and Security for Next Generation Networks, 2008, page 217 et seq.

18 For a brief history of the Internet, including its military origins, see: Leiner, Cerf, Clark, Kahn, Kleinrock; lynch, Postel, Roberts, Wolff, "A Brief History of the Internet", available at: http://www.isoc.org/internet/history/brief.shtml

19 Lipson, "Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues".

20 Callanan/Gercke/De Marco/Dries-Ziekenheiner, Internet Blocking - Cybercrime Response in Democratic Societies, 2009.

21 Telenor Norge: Telenor and KRIPOS introduce Internet child pornography Filter." Telenor Press Release, 21 Sep 2004; Clayton, Failures in a Hybrid Content Blocking System in: Privacy Enhancing Technologies, 2006, page 79; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008, page 46 et seq.; The Cybercrime Convention Committee (T-CY), Examples of how the private sector has blocked child pornograpyh sites, T-CY (2006) 04, page 3.

22 Swedish Providers are using a tool called „Netclean". See Netclean Pro Active, available at: http://www.netclean.com/documents/NetClean_ProActive_Information_Sheet_EN.pdf; Telenor and Swedish National Criminal Investigation Department to introduce Internet child porn filter, Telenor Press Release, 17 May 2005, available at: http://press.telenor.com/PR/200505/994781_5.html; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008, page 59 et seq.; The Cybercrime Convention Committee (T-CY), Examples of how the private sector has blocked child pornograpyh sites, T-CY (2006) 04, page 3; Edwards/Griffith, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008, page 6.

23 Sieber/Nolde, Sperrverfuegungen im Internet, 2008, page 55; Schwarzenegger, Sperrverfuegungen gegen Access-Provider in: Arter/Joerg, Internet-Recht und Electronic Commerce Law, page 250.

24 Edwards/Griffith, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008, page 4; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008, page 64 et seq.; The Cybercrime Convention Committee (T-CY), Examples of how the private sector has blocked child pornograpyh sites, T-CY (2006) 04, page 3; Eneman, A Critical Study of ISP Filtering of Child Pornography, 2006, available at: http://is2.lse.ac.uk/asp/aspecis/20060154.pdf

25 Lonardo, Italy: Service Provider's Duty to Block Content, Computer Law Review International, 2007, page 89 et seq.; Edwards/Griffith, Internet Censorship and Mandatory Filtering, NSW Parliamentary Library Resarch Service, Nov. 2008, page 6 et seq.; Sieber/Nolde, Sperrverfuegungen im Internet, 2008, page 54.

26 Clayton/Murdoch/Watson, Ignoring the Great Firewall of China, available at:

http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf; Pfitzmann/Koepsell/Kriegelstein, Sperrverfuegungen gegen Access-Provider, Technisches Gutachten, available at: http://www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrvervuegungen.pdf; Sieber/Nolde, Sperrverfuegungen im Internet, 2008, page 53; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008, page 73;

27 Sieber/Nolde, Sperrverfuegungen im Internet, 2008, page 53; Stol/Kaspersen/Kerstens/Leukfeldt/Lodder, Filteren van kinderporno op internet, 2008, page 73.

28 Sieber/Nolde, Sperrverfuegungen im Internet, 2008, page 55

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

30 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.

31 Regarding the need for international cooperation in the fight against Cybercrime, see: Putnam/Elliott, “International Responses to Cyber Crime”, in Sofaer/Goodman, “ Transnational Dimension of Cyber Crime and Terrorism”, 2001, page 35 et seq; Sofaer/Goodman, “Cyber Crime and Security – The Transnational Dimension” in Sofaer/Goodman, “The Transnational Dimension of Cyber Crime and Terrorism”, 2001, page 1 et seq.

32 National Sovereignty is a fundamental principle in International Law. See Roth, “State Sovereignty, International Legality, and Moral Disagreement”, 2005, page 1.

33 See Gercke, “The Slow Wake of A Global Approach Against Cybercrime”, Computer Law Review International 2006, 142. For examples, see Sofaer/Goodman, “Cyber Crime and Security – The Transnational Dimension”, in Sofaer/Goodman, “The Transnational Dimension of Cyber Crime and Terrorism”, 2001, page 16.

34 See: Lewis, “Computer Espionage, Titan Rain and China”, page 1, available at: http://www.csis.org/media/csis/pubs/051214_china_titan_rain.pdf

35 Gercke, “Understanding Cybercrime: A Guide for Developing Countries”, ITU 2009, page 71.

36 This issue was addressed by a number of international organisations. The UN General Assembly Resolution 55/63 points out: “States should ensure that their laws and practice eliminate safe havens for

those who criminally misuse information technologies". The full text of the Resolution is available at: http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf. The G8 10 Point Action plan highlights: "There must be no safe havens for those who abuse information technologies".

37 Regarding the impact on computer forensic and criminal investigations, see: See Huebner/Bem/Bem, "Computer Forensics – Past, Present And Future", No.6.

38 With regard to the importance of encryption technology see: OECD Report on Background and Issues of Cryptography Policy, 2007; The importance of encryption is further highlighted by the fact that 74 per cent of respondents of the 2006 E-Crime Watch Survey mentioned encryption technology as one of the most efficient e-crime fight technologies. For more information, see: "2006 E-Crime Watch Survey", page 1.

39 Regarding the consequences for the law enforcement, Denning observed: "The widespread availability of unbreakable encryption coupled with anonymous services could lead to a situation where practically all communications are immune from lawful interception and documents from lawful search and seizure, and where all electronic transactions are beyond the reach of any government regulation or oversight. The consequences of this to public safety and social and economic stability could be devastating". Excerpt from a presentation given by Denning, "The Future of Cryptography", to the joint Australian/OECD conference on Security, February, 1996. Regarding practical approaches to recover encrypted evidence see: Casey "Practical Approaches to Recovering Encrypted Digital Evidence", International Journal of Digital Evidence, Vol. 1, Issue 3.

40 Regarding the use of cryptography by terrorists, see: Zanini/Edwards, "The Networking of Terror in the Information Age", in Arquilla/Ronfeldt, "Networks and Netwars: The Future of Terror, Crime, and Militancy", page 37Flamm, "Cyber Terrorism and Information Warfare: Academic Perspectives: Cryptography", available at: http://www.terrorismcentral.com/Library/Teasers/Flamm.html