

Centre for Cybercrime Studies

Technological, organisational and legal expertise united

contact: Wouter Teepe, w.teepe@cs.ru.nl <http://www.cycris.nl>



v0.7.5 5/12/07 WT

Abstract:

This document forms the foundation for an academic expertise centre in cyber crime in the Netherlands, as a joint endeavour between the universities of Nijmegen and Tilburg (initially). The centre aims to bring together technical, organisational and legal expertise and research activities in the area of cybercrime in order to produce up-to-date scientific output and (contract) evaluations and advice.

1. Introduction

Computers, networks and mobile communication have become entangled in everyday life. Our society has become increasingly connected and dependent on its ICT-infrastructure in business, public administration and personal life. As a result of this dependence, a whole spectrum of punishable behaviour has come into existence. The rapid progress in this field makes it hard not only to maintain technological countermeasures, but also makes it hard for legislatures and law enforcement to keep up with the latest developments. The Dutch Computer Crime Act was well-prepared before it was introduced in 1993, but it soon became outdated because it failed to address an essential aspect of the new technology: communication via networks. In September 2006, the criminal law was updated by the Computer Crime II Act, and it is expected that repeated adjustments and modifications will be required to reflect future technological advancements and developments.

A related issue in this highly technological field is that legislative bodies and law-enforcement agencies have difficulty in recognizing and exploiting the technical know-how that is required to react adequately to the developments. The appearance of relevant software types such as viruses, worms, Trojans, botnets, adware and spyware are notoriously difficult to classify legally, and the combating of malicious software ("malware") is not as effective as one would desire.

Also, new types of identity fraud are emerging, which rely on phishing, pharming and other techniques of social engineering. Often, it is unclear how these new forms of misbehaviour should be defined and classified. In practice, one calls such activities identity theft, but this is an unfortunate term, given the intrinsic immateriality of information which cannot as such be 'stolen'. The principle of legality, which prevents the use of reasoning by analogy in criminal law and requires penal provisions to be precise, implies that such a confusion of concepts is not nit-picking but a matter of the utmost practical importance.

Conversely, technology should not only be addressed as the subject of misbehaviour, but also as a valuable means for law enforcement (cf. *Politie in ontwikkeling*, 2005, and *Spelverdeler in de opsporing*, 2004, both by the Dutch Council of Chief Superintendents of Police). Classical criminal investigations should be enhanced, and in some particular cases even be replaced by digital criminal investigation and forensics.

We consider the following research subjects to be relevant, grouped by focus:

Technological:

- The (unnoticed) monitoring of certain message streams in search of suspected and alarming information;
- Forensic search in structured information collections on the hard disks of seized computers (data mining), for example for modus operandi information;
- Forensic search in unstructured information collections, such as text on the Internet (text mining);
- Link analysis and traffic analysis to identify relations between suspects;
- Issues in information modelling and architecture and ownership of data bodies subject to data mining;

Legal:

- Identity management in the context of fraud and criminal investigations, for example with revocable privacy (e.g. requiring more identification in case of a conviction for internet frauds);
- Trans-border issues;
- The role of ICT experts in the interpretation of digital evidence in court;
- Effectivity and proportionality questions in relation to (aspects of) new and existing legislation;
- Formalization of (required) security properties, both in legal and in logical terms, and the interplay between them;
- The interpretation of legislation regarding investigative privileges;

Organisational:

- The exchange and handling of digital evidence in the whole chain of criminal prosecution, including the preservation of digital evidence;
- The organisational and legal aspects of automated bulk processing of the digital gathering of evidence;
- Risk management and economic incentives and drivers of prevention of and protection against cybercrime;
- Coordination between stakeholders in the public and private sector;
- The effectivity of abusedesks;

General:

- Auditable, more privacy-friendly lawful interception technology;
- Analysis of commonly used technology for attacks, protection and prevention (existing vulnerabilities and possible solutions);
- Threat/fraud analysis to establish how much cybercrime actually occurs;

This list is not static, but may be expected to change in due course under the influence of technical, legal and societal developments.

These issues require both fundamental research and practical know-how and advice. The fundamental research is needed to capture actual technical and non-technical developments in order to develop and maintain clear, useful legal and technical terminology and definitions. The required practical advice is addressed mainly at the legislator and judicial authorities.

The research performed will be multidisciplinary and will cover technical, legal, and social science. There is currently a gap in the multidisciplinary study of cybercrime which Cycris aims to address.

2. Domain coverage

The area of expertise of Cycris is Cybercrime. As such, we have not chosen the traditional term “computer crime”, which mainly suggests acts performed in and with computers. Cybercrime, in contrast, also includes networks and (mobile) communication explicitly in its

domain, and also stresses that the phenomenon addressed is international, as it does not take heed of territorial borders.

In practice this boils down to criminal behaviour related to ICT. For ease of communication, we will consider the terms cybercrime, computer crime and ICT crime as synonyms for this broad class of criminal behaviour.

To provide an initial classification of cybercrime, the distinction can be made between cybercrime in the narrow sense and cybercrime in the broader sense. Cybercrime in the broader sense has a further subdivision in crime where the computer (and the network) is a tool, and crime where the computer (and the network) is only its environment or context. This is depicted in Figure 1.

	cybercrime in the narrow sense	cybercrime in the broad sense	
role of the computer	computer as the object <i>the computer, or information stored on the computer, is the subject or target of the crime</i>	computer as a tool <i>the computer, or information stored on the computer, constitutes an important tool for committing the crime</i>	computer as the environment or context <i>the computer, or information stored on the computer plays a non-substantial role in the act of crime, but do contain evidence of the crime</i>
examples	hacking computer sabotage (D)DoS-attacks virtual child pornography	computer fraud forgery distribution of child pornography	murder bank robbery drugs trade

Figure 1. Classification of cybercrime

It is obvious that the first column is covered by the activities of Cycris, but also the second and third column will get substantial attention. Moreover, it should be noted that this classification is only preliminary, and a thorough combat by law enforcement bodies of cybercrime will require a more elaborated and refined model than the one described here. It is the academic aim of Cycris to facilitate this by providing proper notions, techniques and tools (see also the research questions in Section 3).

From this classification, two large clusters of issues arise, which differ in kind and focus, that will form the two major pillars of the Centre for Cybercrime Studies:

1. investigation and analysis of 'hardcore' cybercrime, such as botnets, hacking, and viruses;
2. investigation and analysis of the role and use of ICT in the combat against crime in general.

The first pillar will focus mainly on finding the right mix of measures to combat hardcore cybercrime effectively. The second pillar will focus mainly on developing and implementing measures that use ICT to combat crimes in which digital evidence may be relevant. One key issue here – but not the only one – is to find a justifiable balance between the privacy of citizens and effectivity of law enforcement

These two pillars will be addressed from the technical, organisational and legal perspective. From the technical perspective, the focus lies on the tools and technologies available to cyber criminals, potential victims and law enforcement for the execution, protection against and prosecution of cybercrime, and digital forensics. From the organisational perspective, the focus lies on the cooperation between and responsibilities of all stakeholders in the field of cyber crime. From the legal perspective, the focus lies on criminalisation of punishable activities targeted at computers (largely related the field of substantive law) and on establishing investigation and prosecution powers (largely related to the field of procedural law).

The area of coverage corresponds with the Convention on Cybercrime of the Council of Europe. This correspondence is intentional, as it covers a broad set of punishable behaviour and investigation powers about which there is a reasonable level of international consensus. The following matters of substantive law are primarily of interest:

- Illegal access to computer systems (art. 2);
- The interception of confidential communication by electronic means (art. 3);
- Data modification and interference (art. 4);
- System sabotage and interference (art. 5);
- Misuse of devices for crimes as described in articles 2–5 (art. 6);
- Computer-related forgery and fraud (art. 7, 8);
- Child pornography (art. 9) and racism (protocol to the Convention on Cybercrime);

- Infringements of copyright and related rights (art. 10);
- Other punishable activities not regulated as such in the Cybercrime Convention, such as cybersquatting, spam and identity 'theft'.

Secondly, the following matters of procedural law are of interest:

- Preservation of stored computer data (art. 16, 29) and of traffic data (art. 17, 30);
- Access to stored computer data (art. 19, 31);
- Cross-border network search (art. 32);
- Collection of traffic data (art. 20, 33);
- Interception of content data (art. 21, 34).
- 24/7 network of contact points to provide international assistance (art. 35).

All these points fall within the larger framework for Cycris, but they require continuous interpretation in our rapidly changing network society.

Terrorism and cyber-terrorism will not be a particular special focus of Cycris. Cycris does not focus on the goals and motivation that underlie the cybercrimes committed. Additionally, the technical means available to the terrorist are not intrinsically different from those available to the 'ordinary' criminal. As such, the research results of Cycris can by and large be applied similarly to investigating cyber-terrorism.

3. Ambition

Cycriis aims to connect technical knowledge with legal knowledge concerning cybercrime, both on the academical and on the practical level. The underlying aim is to create new insights in the theory and practice of cybercrime.

The people involved in Cycriis are independent scientists from various backgrounds, having no role in actually combating cybercrime. The output of their research work may sometimes help cybercrime fighters, and sometimes criticize them – scientific integrity is a key value in (contract) research at Cycriis.

From the technical perspective (ICIS Nijmegen), the multidisciplinary research creates insights in the technical possibilities and impossibilities for committing cybercrime but also for analyzing and combating it. As to combating cybercrime, prevention, detection and the preservation of digital evidence are relevant.

From the legal and organisational perspective (TILT Tilburg, Institute for Law Nijmegen), the research provides insights in the possibilities and impossibilities of the regulation of technology and the regulation by means of technology, insights in the actual incidence of cybercrime, and its impact on victims, citizens and government. On the law-enforcement side, the research will help to set priorities, bring relevant expertise together and will bridge the gap between theory (law, concepts) and practice.

Altogether the research will offer insights that can be used to improve legislation, that will help to prevent and to prosecute cybercrime, and to assist victims of cybercrime.

Once the centre is finally established it may also develop its own teaching programme, for instance via a joint master programme in cybercrime.

4. Research Questions

The main question that the Centre for Cybercrime Studies (Cycriis) wishes to address is:

Based on a scientific analysis, what combination of instruments (including legislation, regulation, social norms, economic and technical measures) can best be applied in order to keep cybercrime under control, in terms of prevention, detection and prosecution?

Practical research questions are, grouped by focus:

Technological:

- What technologies are used by cyber criminals? (This is a continuous research question with a moving target);
- What technologies can be used to prosecute and convict offenders of cybercrime?
- What technologies can be used to detect offenders of cybercrime, and to preserve digital evidence?
- Is it possible to adapt the technological infrastructure in such a way that cybercrime can be more easily detected and/or combated?

Legal:

- What classification of techniques (e.g. social engineering, malware, network breaches) is useful for the prevention and prosecution of cybercrime?
- Do the concepts distinguished in the law match the observed punishable forms of behaviour?

Organisational:

- Which parties are subject to what risks, and how should these parties guard themselves against these risks?
- Where should the (moral, legal) liability for insufficient protection against cybercrime reside?

General:

- What is the precise kind and extent of the distinguished forms of misbehaviour (both factually and in the perception of involved stakeholders)?
- How effective are the various instruments (including legislation, regulation, social norms, economic and technical measures) that can be applied to prevent and combat cybercrime?
- In what way can a proper balance be found between the interests of law enforcement and the interests of individual citizens (privacy, ease of use, cost)?
- To what extent are confidentiality-improving technologies (e.g. encryption, anonymisation) profitable or troublesome for combating cybercrime?

Where the required technological means are lacking, projects will be entered upon to develop such means, or otherwise ideas and design criteria for such means.

5. Involved research groups

The following research groups and people are involved in Cycris.

Radboud University Nijmegen

ICIS – Institute for Computing and Information Sciences

Security of Systems, especially

dr. Jaap-Henk Hoepman

prof.dr. Bart Jacobs

dr. Wouter Teepe

prof.dr. Eric Verheul

Information and Knowledge Systems, especially

dr. Patrick van Bommel

prof. Cornelis Koster

prof. dr. Theo van der Weide

Institute for Law

Criminal Law Institute (Sectie Straf- en Strafprocesrecht), especially

prof.mr. Ybo Buruma

mr. Martine van der Staak

Tilburg University

TILT – Tilburg Institute for Law, Technology, and Society, especially

prof.dr. Bert-Jaap Koops

dr. Ronald Leenes

dr. Maurice Schellekens

6. References

- Convention on Cybercrime, ETS 185, Budapest, 23.XI.2001.
- Koops, B.J. & Prins, J.E.J.. Misbruik van technische hulpmiddelen: een beschouwing over de te ver gaande regelingen in het Cybercrime-verdrag en de Auteursrechtenrichtlijn, *Computerrecht*, 59-67, 2004.
- Openbaar Ministerie, Perspectief op 2010, Den Haag, 2006
- Raad van Hoofdcommissarissen, *Politie in ontwikkeling - Visie op de politiefunctie*, NPI, Den Haag, May 2005.
- Raad van Hoofdcommissarissen, *Spelverdeler in de opsporing - Een visie op forensische opsporing*, NPI, Den Haag, december 2004.
- Koops, B.J.. Tendensen in opsporing en technologie. Wolf Legal Publishers, Nijmegen, 2006.
- Jacobs, B.P.F. De Menselijke Maat in ICT. Electronic publication (available via <http://www.cs.ru.nl/~bart>).
- Dasselaar, A.. Handboek digitale criminaliteit. Van Duuren Media, Culemborg, 2005.
- D.E. Denning, *Information Warfare and Security*, Addison-Wesley Longman Ltd., 1999.
- Parker, D.B., *Fighting Computer Crime*, New York 1983.
- Brenner, S.W., 'Distributed Security: Moving Away From Reactive Law Enforcement', *International Journal of Communications Law & Policy* 2004 (9).
- Social networking study shows cybercrime risk, *Network Security*, Volume 2006, Issue 11, November 2006
- W. Chung, H. Chen, W. Chang and S. Chou, *Fighting cybercrime: a review and the Taiwan experience*, *Decision Support Systems*, Volume 41, Issue 3, March 2006.
- Russell G. Smith, Peter Grabosky & Gregor Urbas, *Cyber Criminals on Trial*, Cambridge University Press 2004.
- R.W. Taylor, T.J. Caeti, D. Kall Loper, E.J. Fritsch and J. Liederbach, *Digital Crime and Digital Terrorism*, Pearson Prentice Hall, 2006.
- David S. Wall (ed.), *Crime and the Internet*, London: Routledge, 2001.
- David S. Wall (ed.), *Cyberspace Crime*, Ashgate 2003.
- David S. Wall (2007 - forthcoming), 'Policing Cybercrime: Situating the public police in networks of security in cyberspace', *Police Practice and Research: An International Journal*, vol 8, no. 2.