CYBERCRIME: AN ANNOTATED BIBLIOGRAPHY OF SELECT FOREIGN-LANGUAGE ACADEMIC LITERATURE

An Annotated Bibliography Prepared by the Federal Research Division,
Library of Congress
under an Interagency Agreement with the
National Institute of Justice

November 2009

Researchers: *Glenn Curtis*
Ronald Dolan
Seth Elan
Noël Ivey
Carl Minkus
Eric Solsten
Taru Spiegel
Tomoko Steen

Project Manager: Alice R. Buchalter

Federal Research Division
Library of Congress
Washington, D.C. 20540–4840
Tel: *202–707–3900*
Fax: *202–707–3920*
E-Mail: *frds@loc.gov*
Homepage: *http://www.loc.gov/rr/frd/*

✯ 61 Years of Service to the Federal Government ✯
1948 – 2009

PREFACE

This annotated bibliography reviews the findings of major academic research studies on the prevalence of cybercrime and government efforts to stem its escalation. This bibliography is limited to research published from 2000 to 2008 in the native languages of select countries chosen by the National Institute of Justice—Chinese, Dutch, French, German, Italian, Japanese, Korean (Republic of Korea), Russian, Swedish, and Ukrainian. This research is categorized into several subtopics: cybercrime practices defined; cybercrime tools and methods; cybercrime differentiated from traditional crime; cybercrime's threat to government data systems; the link to terrorism; privacy protection; government and law enforcement response; and relevant laws and conventions. In many of the selected countries, critical analyses of the major issues relative to cybercrime have been published by government agencies and non-academic research institutes. Because of the importance of their findings, these studies have been included in this report as well. An appendix provides additional source material identified during the course of research.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This bibliography evaluates major academic research studies on the prevalence of cybercrime and government efforts to stem its escalation, written in Chinese, Dutch, French, German, Italian, Japanese, Korean (Republic of Korea), Russian, Swedish, and Ukrainian. The research studies define the various types of information technology–related crime, or cybercrime; discuss the ways in which cybercrime is uniquely different from traditional crime; and consider cybercrime's link to terrorism. The authors discuss the laws and conventions in force to counter cybercrime, evaluating their effectiveness. They assess the response of law enforcement to the escalation of cybercrime and the preparedness of government agencies to respond to the threats that cybercrime activities pose. In addition, the studies comment on how to achieve a balance between the governments' need to monitor the sharing of personal data and the obligation to protect intellectual property rights and the citizens' right to privacy.

Cybercrime Defined

Researchers studying the scope of this type of criminal activity in various countries have framed a definition of the term itself, as well as identifying the major illegal practices that constitute cybercrime. Myriam Quéméner, evaluating French and European Union law targeting cybercrime, defines cybercrime as criminal activities conducted in cyberspace by means of Internet technology. These crimes fall into two categories: 1) those involving unauthorized access to data and systems for criminal purposes, and 2) those involving fraud, falsification, diversion of funds, obtaining illicit content, or defamation via online services. The report of the Swedish National Council for Crime Prevention on the rise of information technology–related crime identifies, as the most common types of cybercrime, the introduction of viruses into a computer system, external and internal computer intrusion, manipulation of data, information theft, and fraud.

In his research on cybercrime and cyberterrorism in Russia, A. Shchetilov includes in his definition of cybercrime all types of crime that involve perpetrators' infringement in the telecommunications sphere. Shchetilov identifies three specific types of cybercrime: illegal access to information stored in global computer networks; crimes using information in forms other than those that are computer-based; and crimes involving the distribution of harmful

computer programs. S. L. Katayev's research concludes that two types of cybercrime are prevalent in Ukraine: the use of computers as a tool to help criminals smuggle people and illegal goods, or for other conventional criminal activities, and the use of computers to assist individuals in tax evasion.

In their study of the characteristics of Internet crime in China, Sun Tianzhu and Cao Peizhong state that the Chinese definition of computer crime includes those crimes that use computers as the main tool, as well as those that have computer assets as their primary target. These crimes, which use the highly technical methods of the virtual world, are premeditated intellectual crimes carried out with specialized knowledge of computers. In his study of the legal issues of cybercrime in China, Chen Junjing's definition of cybercrime includes, but is not limited to, the following activities: fraud, Internet pornography and sexual harassment, trafficking and sale of prohibited goods, damage to people's reputations and invasion of their privacy, and manufacture and dissemination of computer viruses.

Akira Watanabe's study of the recent increase in cybercrime cases in Japan notes that cybercriminals are accessing computers for the purpose of prostitution, drug dealing, password theft, unauthorized transfer of funds, and distribution of copyrighted materials. In his discussion of crimes against private users of the Internet in South Korea and Germany, Yong-bong Yu cites particular crimes: spamming, cyber stalking, hacking, infecting computers with viruses, illegal online gaming, and capturing screen images for illegal purposes.

Cybercrime Tools and Methods

Cybercriminals are using numerous illegal tools: *keylogging*—using software or devices to secretly monitor and record keystrokes, enabling espionage activities or the harvesting of personal data; *distributed denial of service* (DDoS)—inundating computer system resources with tasks sufficient to render them unavailable to authorized users; *pharming*—directing traffic from a legitimate Web site to a site controlled by a criminal hacker; *phishing*—illegally accessing an individual's financial data to capture online banking and financial information; and, most recently, *botnets*—networks of infected machines, usually managed by a single command center, that are capable of causing serious damage to networked systems and enabling large-scale identity theft. Hackers obtain botnets commercially, using them to access bank accounts.

In her discussion of the threat of cybercrime to Russian society, Vanessa Vitaline identifies keylogging as a general threat and notes that DDoS attacks are a threat to companies and governments. Vitaliy Vekhov, in his analysis of Russian cybercrime, confirms the rapid growth, over the past 10 years, of DDoS crimes. Antonio Apruzzese notes that digital identity theft, also known as phishing, has become one of the most lucrative illegitimate businesses in Italy. Rodion Nasakin, in his study of the illegal use of personal information in Russia, notes the rapid growth of phishing since 2000, with phishers successfully tricking customers into revealing passwords and personal identification numbers, thereby enabling access to bank accounts and credit cards. A 2008 report of the Swedish Emergency Management Agency notes that phishing has troubled Sweden's banks since 2006. A. Poller analyzes the vulnerability of social network platforms—Internet-based applications in which users model their relationships to other people, e.g., facebook—and concludes that these applications are a potential target of cybercrime.

Cybercrime Differentiated from Traditional Crime

Cybercrimes, uniquely different from traditional crimes, are often harder to detect and prosecute. The Swedish Emergency Management Agency's 2008 report, "Information Security in Sweden: Situational Assessment," observes that criminal activity on the Internet has become progressively more sophisticated. Perpetrators carry out cybercrimes through small, targeted Internet attacks, as well as launching significant attacks using large networks of commercially leased, hijacked computers.

Chen Junjiing, researching the legal issues of cybercrime in China, concludes that these crimes are more widespread than traditional crimes and are increasing at a faster rate. Furthermore, cybercrime does greater damage to society than traditional crime and is more difficult to investigate. In her study of the use of cybercrime for fraudulent financial activity in France, Vanessa Vitaline identifies typical characteristics of cybercrime: it is inexpensive, fast, anonymous, and has global impact. Its perpetrators use remote intervention to carry out their crimes, recruiting experts in data processing and networking to assist them in activities designed to corrupt computer systems. A. I. Zhurba also notes that, in Ukraine, remote crimes constitute the majority of computer crimes. Perpetrators of these crimes often commit the crime at a place different from the location where the victim sustains harm or where the damage occurs.

Leo Stilo, reporting the results of a 2006 IBM study of computer crime in business, notes that 46 percent of Italian executives believe that computer crime is more damaging financially than traditional crime. In a report published for the Ukrainian Center for Research on Problems of Computer Crime, N. N. Akhtyrskaya warns that criminal syndicates tend to commit sophisticated cybercrimes, with multiple levels of criminal activity, and that the process of investigating these crimes is typically fragmentary, complex, and fraught with false leads. In another report written for the Ukrainian research center, Vitaliy Vekhov concludes that, because many companies require timely Internet access to conduct business, when cybercriminals overload, and thereby cripple, a company's Web site or computer system, using the technique of DDoS, the victimized company is willing to meet extortion demands in order to repair the blockage.

Threat to Government Data Systems

In addition to the threats that it poses to individuals and companies, cybercrime may also jeopardize government systems and public infrastructure. Bernadette Ferchaud reports the activities of a 2002 conference on new threats to economic intelligence, sponsored by the French Society of Competitive Intelligence Professionals. At this conference, participants identified cybercrime aimed at the illegal acquisition of privileged economic data as an emerging threat facing (in order of severity) government agencies, businesses, and individuals.

Government researchers, particularly in Sweden, a country that suffers from one of the highest incidents of cybercrime in the world, acknowledge the vulnerabilities of government systems in the face of the threat to information security, both within their own countries and throughout the world. "Information security in Sweden—An overview," an official report of the Swedish government, urges cooperation among all parties involved in information protection. The report warns both service providers and users to protect their data systems from a wide variety of threats: physical threats, weapons, and viruses, some of which are widespread enough to constitute epidemics.

A 2008 report by the Swedish Emergency Management Agency concludes that Sweden is inadequately prepared to protect itself against major infrastructure attacks. Computer and network failures have affected the systems of the Swedish government, including the judiciary; Teracom, radio, and television broadcasters; and medical care providers. Junk mail (spam) and

viruses constantly bombard computer systems and networks. In a 2007 report, "Sweden's preparedness against net attacks," the Swedish Emergency Management Agency warns that Sweden is vulnerable to threats of the most severe kind, including the sabotage of critical infrastructure, such as the supply of electricity or water. Both the Swedish National Audit Office and the author agency note shortcomings in the way that government authorities responsible for crucial infrastructure handle their own information security. These government entities demonstrate that they do not understand their systems' vulnerability to cyber attack.

Link to Terrorism

Researchers in Italy and Ukraine, observing that terrorists are able to use the tools of cybercrime to achieve their goals, urge governments to focus attention on the new phenomenon of cyberterrorism. Arije Antinori, in his analysis of the Internet-based economy, notes that traditional terrorist groups are taking advantage of the new models of social deviance that cyberspace offers. In a 2002 report prepared for the Center for Research on Problems of Computer Crime in Ukraine, Vladimir Golubev and Timofey Saymarly describe the recent development of cyber war as a key weapon of international terrorist groups. Cyberterrorist attacks, which are "planned, motivated attacks on information processed by computer, or on a computer system or network," may occur either directly or from a remote location. The authors believe that remote attacks, which target specific systems or servers from afar, are more dangerous than direct attacks, because they may have global consequences. In his 2001 report, also prepared for the Ukraine research center, A. Shchetilov concludes that the goals and methodology of cyberterrorists are the same as those of conventional terrorists: both conduct information wars, propagating their own views as broadly as possible. The cyber world is ideal for terrorists, because the source of attack is much more difficult to identify than in traditional forms of terrorism.

Privacy Protection

Governments face a dilemma in balancing the need to gain access to personal data—both to prevent and to prosecute cybercrimes—with the need to protect individual privacy and civil liberties. Most of the academic research in the Netherlands has focused on this paradox. Dutch

law professor Ybo Buruma argues that Dutch laws allowing government agencies to access citizens' financial, telecommunications, and other personal data, in the course of investigating cybercrime and other criminal offenses, have not greatly threatened personal privacy. Buruma states that these laws are of limited effectiveness and grant the government much less authority than critics allege. He does, however, justify the legal use of data collected by government security agencies in the course of criminal investigations, arguing that the value of enhanced security outweighs the moderate reduction in personal privacy.

Bart Jacobs and Wouter Teepe, both professors of computer science at universities in the Netherlands, examine the controversy surrounding the Dutch government's use of information technology to collect and store personal data. They note that, although this practice creates many opportunities to misuse citizens' personal information, measures to prevent the misuse of this information could undermine effective data collection and processing. Writing in 2006, while the Council of Europe was implementing its directive on data retention (Directive 2006/24/EC), three Dutch lawyers—Ronald Leenes, Paul De Hert, and Jos Vander Velpen—evaluate the impact of this directive on Dutch society. The directive requires providers of communications networks and services to save data on individual usage, so that public authorities can access such data for use in detecting, investigating, and prosecuting serious crimes. However, the authors suggest that the directive could lead to violations of citizens' privacy and abuses by law enforcement agencies. University of Tilburg professors Anton Vedder, Leo van der Wees, and Bart-Jaap Koops raise concerns that the availability of individuals' personal data and the government's access to that data has diminished citizens' privacy and increased the risk of authorities treating a person as a suspect without probable cause. They urge greater transparency in the government's investigative and judicial powers.

In Japan, Osamu Sakuma, writing on measures for the prevention of cybercrime, notes that Internet providers have difficulty collaborating with the government to stop cybercrime, because Japanese privacy laws aimed at protecting users often protect those who are committing cybercrimes. In their 2004 article, Sun Tianzhu and Cao Peizhong, reporting that the People's Republic of China is in the process of drafting a new Internet activity law, caution that China should carefully craft the new law, so that it limits cybercrime without inhibiting lawful commercial activity and without infringing on the personal rights, privacy rights, and intellectual property rights of citizens and corporations.

Government and Law Enforcement Response

In recognition of the growing sophistication and frequency of cybercrime attacks, foreign governments and their law enforcement agencies have taken steps, with varying degrees of success, to prevent and to prosecute cybercrime. Many researchers who have studied the effectiveness of government intervention are critical of these efforts. Sun Tianzhu and Cao Peizhong, analyzing the characteristics of Internet crime in China, conclude that the Chinese government has been relatively slow to monitor, regulate, and control Internet crime.

The authors of a series of articles published by the Ministry of Justice of the Netherlands argue that the power of Dutch authorities to undertake electronic surveillance and to access personal data when investigating cybercrime is insufficient for policing some types of information technology–related crimes, such as computer-based attacks on public utilities and other public infrastructure. However, Corien J. E. J. Prins finds that, in the Netherlands, the use of government security measures, such as biometrics and centralized information databases, has resulted in a high rate of error in identifying individuals, and that criminals use these same measures to perpetrate identity fraud and other crimes. He cautions that, rather than recognizing the vulnerabilities of these security measures, Dutch politicians overemphasize their security and their administrative benefits.

Vitaliy Vekhov discusses the rapid increase in Russia in crimes using plastic cards, and notes that investigation of these crimes is not keeping pace with the rate of criminal activity. He concludes that Russia has an insufficient number of personnel qualified to investigate, assemble evidence, and prosecute crimes involving plastic cards. In addition, Russia has a high volume of card-related cases requiring presentation in court. Because they have an insufficient understanding of the legal status of cases involving plastic cards, of the potential for criminal misapplication of these cards, and of the role that misuse of cards plays in legal cases, police and prosecutors often encounter difficulties in investigation during the preliminary stages of mounting this type of criminal case.

Under the Swedish civil law system, controlling cybercrime—from cases of compromised personal identity to those that threaten national security—is largely the responsibility of the Swedish government. According to a report by the Swedish Defence Research Agency (Totalförsvarets forskningsinstitut—FOI), pursuant to legislation enacted in 2001, Sweden has appointed the Swedish Emergency Management Agency, the National

Defence Radio Establishment, the National Post and Telecom Agency, and the Swedish Defence Matériel Administration responsible for the respective areas of intelligence collection, technological competence, management of information technology incident reports, and the establishment of Sweden's Scheme for Evaluation and Certification. However, "Government management of information security in national administration," a 2007 report of the Swedish National Audit Office, concludes that, because of a lack of oversight and an incomplete understanding of the various information security requirements and regulations, Swedish government agencies have failed to provide adequate protection for their information technology systems.

The governments of Italy and Japan have taken more positive actions to counter cybercrime. A paper by Andrew Livesley and Koichi Kurokawa discusses the work of the electronic/cybercrime prevention team of Japan's Serious Organized Crime Agency (SOCA). This branch of SOCA is divided into five different groups that collaborate with one another on many of their activities: Crime Benefit, Electronic Crimes, International, Crime Technology, and Prevention. Antonio Appruzzese notes that, in response to Italy's rise in large-scale identity theft using various illegal computer activities, the Italian State Police created the Servizio Polizia Postale e delle Comunicazioni (Postal and Communication Police), a new agency specializing in combating this type of cybercrime. Furthermore, Domenico Vulpiani points out that the Italian Servizio Polizia Postale e delle Comunicazioni (Postal and Communication Police) recently introduced innovations to combat the risk of computer crimes and computer-related crimes, innovations that include the establishment of the Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche Informatizzate (National Center Against Information Crime for the Protection of the Critical Information Infrastructure); the Child Exploitation Tracking System, which fights online pedophilia; and the first online police station—the Online Police Office for Security(OLPS).

Laws and Conventions

The countries selected for this study have adopted laws to prevent and prosecute cybercrime activities. In addition, many of these countries are parties to international conventions that address cybercrime. However, analysts continue to debate the efficacy of these

laws. Most researchers conclude that these countries will require new legislation if they are to address the challenges of escalating cybercrime successfully.

In their 2004 article, Sun Tianzhu and Cao Peixhong, acknowledging the inadequacy of the People's Republic of China's laws countering cybercrime, report that China is drafting new legislation regarding Internet activity. Jan Vetter's 2002 study of gaps in German law regarding Internet crime concludes that Germany's law has not kept pace with the rapidly evolving techniques used in committing Internet crimes. In a 2008 article, Hajo Koppen notes that German laws addressing computer crime are more than 20 years old. Yann Padova, an official assigned to the French National Assembly, in his 2002 overview of the battle against cybercrime in France, concludes that French laws are inadequate for dealing with cybercrime, and that the French police do not have suitable instruments at their disposal for combating the threat.

Studies by professors of law and computer science in the Netherlands critique Dutch criminal laws that allow authorities to examine citizens' financial and personal data in the course of cybercrime investigations. Furthermore, Corien J. E. J. Prins and Bart-Jaap Koops argue that Dutch law provides excessive punishments for minor cybercrime and copyright offenses, but does not sufficiently punish major offenses, such as hacking and data manipulation.

In a 2001 report for the Center for Research on Problems of Computer Crime, Ukraine, M. V. Gutsalyuk analyzes the growth of various forms of cybercrime in Ukraine, discussing the legal response. He draws a direct link between Ukraine's highly inadequate system of defense against cybercrime and the shortcomings of the country's laws. Gutsalyuk cites a lack of hierarchical, clear, and uniform laws, which has lead to variant legal interpretations, and to the enactment of new regulations and laws that contradict the existing ones. The author notes one recent positive development: Ukraine's Interjurisdictional Scientific-Research Center on Problems of Combating Organized Crime has created the Conception for Reform of Legislation on Information Systems.

Carlo Carlesi's report for the Alessandro Faedo Institute of Computer Science and Technology notes that Italy was among the first European countries to enact legislation to protect computer data and among the first to create a government entity (the Authority for Information Technology in the Public Administration—AIPA) to take responsibility for the protection of data.

In response to the Council of Europe's Convention on Cybercrime and its Copyright Directive (Directive 2001/29/EC), signed in 2001, and the Council of Europe's Directive 2006/24/EC regarding data retention, many countries, including the Netherlands, Sweden, France, Germany, Italy, and Japan, are drafting or have adopted new legislation to comply with the requirements of these agreements. The Swedish Ministry of Justice reported in 2005 that Sweden had signed the Council of Europe Convention in 2001 and an additional protocol in 2003. In a memorandum discussing what issues it should consider in the context of ratifying the 2001 Council of Europe Convention, the Swedish government identifies the need to harmonize Swedish laws regarding punishment of forgery, data interference, child pornography, unlawful use of computers, unlawful monitoring of computer information, and the violation of copyright and related rights.

In his 2007 report for the Swedish Law and Informatics Research Institute on efforts to stem unlawful file sharing, Daniel Westman notes two proposed laws to address this issue. According to the first proposed law, in a case in which perpetrators have used an electronic-service subscription to infringe intellectual property rights, a court may order the provider of the electronic service not to disclose to the intellectual property owner the name of the account subscriber. Under the second proposed law, electronic-service providers may terminate the service of those accounts that perpetrators have repeatedly used to violate copyright law. The Swedish Parliament rejected a similar bill in December 2008.

Writing in 2005, Makoto Ibusuki notes that, in November 2001, Japan also signed the Council of Europe Convention, and that in 2004 the Japanese parliament approved Japan's participation in the Convention. Ibusuki reports Japan's implementation of domestic legislation, pursuant to the Convention's directives and discusses pending cybercrime legislation. In a 2003 article, Tadashi Sakamaki analyzes the changes in Japan's criminal laws since signing the Convention. These laws address key issues, including requests for communication records, requests to provide data regarding a suspected crime, confiscation of media for recording and investigating, and general requests for criminals to cooperate in investigations.

Conclusion

Academic researchers who have evaluated the scope of cybercrime activities and the impact of cybercrime on society agree that this type of crime is global and that it is growing and

diversifying rapidly. These analysts are also concerned that many governments have failed to address cybercrime effectively. In many instances, laws aimed at prosecuting cybercrime are either outdated or in conflict with other criminal statutes. Perpetrators of cybercrime are often more sophisticated in their methods than are the law enforcement agencies that investigate them. Writing about the impact of cybercrime in France, Vanessa Vitaline concludes that, despite countermeasures taken by governments and police authorities, cybercrime continues to grow exponentially, and criminal organizations continue to reap its benefits. M. V. Gutsalyuk, summing up the dimensions of the problem of cybercrime in Ukraine, draws a conclusion that could apply to many of the countries in this study: "There needs to be a coordination between the making of laws on information systems with the real-world requirements of the field, to realize the advantages of electronic communications while ensuring information security both in Ukraine and elsewhere."

CHINESE LITERATURE

Chen Junjing. "Wangluo Fanzui de Falü Wenti Yanjiu" [Study of the legal issues of cybercrime]. Study, People's Court, Qidong, Jiangsu, People's Republic of China, November 11, 2004. http://www.chinacourt.org/public/detail.php?id=138544.

With the current widespread use of computers, the development of the Internet affects every aspect of our society. Although the Internet offers convenience and speed, it brings with it a series of legal problems. After summarizing the concept, characteristics, and structural features of cybercrime, the author discusses specific types of cybercrime. In addition, the article investigates jurisdictional issues that the Internet has caused, citing cases dealing with Internet piracy, as well as other examples, and suggesting possible resolutions of these issues. Finally, the article offers a framework of standards regarding the type of activities that constitute cybercrime and praises some improvements in legislation to address cybercrime.

The author discusses some characteristics that he considers specific to cybercrime, stating that cybercrime is cheaper and more widespread than traditional crime and is increasing more quickly than traditional crime. The author asserts that cybercrime is more interactive and clandestine and more difficult to investigate than traditional crime, and that it does greater damage to society. He argues that, while cybercrime is intentional, like any other type of crime, it is more complex. Types of cybercrime include, but are not limited to, Internet pornography and sexual harassment, fraud, trafficking and sale of prohibited goods, damage to people's reputations and invasion of their privacy, and the manufacture and dissemination of computer viruses.

Although the jurisdiction of a cybercrime is often difficult to determine, the predominant view of Chinese law is that, if the criminal activity—uploading, downloading, or computer use—occurs

in China or if the activity could have an effect in China, the Chinese government considers it criminal activity and claims jurisdiction over that crime.

Li Xing'an. "Lun Wangluo Fanzui" [On cybercrime]. Dissertation, Kyushu University, Japan, May 26, 2005. http://www.law-lib.com/LW/lw_view.asp?no=985.

The Education Ministry of the People's Republic of China sponsored Li Xing'an, an instructor in the Law School of Inner Mongolia University, as an exchange student at Japan's Kyushu University. In this dissertation, he provides a brief history of the Internet and the accompanying rapid growth in cybercrime, comparing Japanese statistics of 1999 and 2000 regarding various types of cybercrime. Li Xing'an describes in detail the different types of cybercrime, including Internet pornography and sexual harassment; trafficking in pirated CDs; trafficking in forbidden items, controlled items, and human organs; selling stolen goods; fraud; defamation of character; hacking into Web sites or e-mail; creating or disseminating computer viruses; Internet gambling; invasion of privacy; forging papers or currency; aiding and abetting certain crimes or imparting criminal methods; and threats, blackmail, and extortion. In addition, he lists seven reasons that cybercrime is difficult to combat:

1) Defects in the Internet itself
2) Widespread software hacking
3) The Internet's cross-border and international nature
4) Abuses in Internet commerce
5) The Internet's indeterminate nature
6) Lack of uniformity in judicial standards
7) The failure of many countries to attack cybercrime aggressively

Sun Tianzhu and Cao Peizhong. "Wangluo Fanzui Tedian ji Zeren Zhuijiu LifaYanjiu" [Research on the characteristics of Internet crime and the responsibility for examining legislation]. *Dongfang fayan* [Eastern legal eye], April 5, 2004. http://www.dffy.com/faxuejieti/xs/ 200404/20040405160634.htm.

The authors of this online article analyze the characteristics of Internet crime, recommending changes in legislation to clarify responsibility for network crimes and to provide better legal protection of China's networks. The Chinese definition of computer crime includes crimes that use computers as the main tool, as well as those that have computer assets as their primary target. Internet crime, which uses the highly technical methods of the virtual world, has several general characteristics:

1) Internet crime is a premeditated intellectual crime carried out with specialized computer knowledge.
2) Internet crime involves a high degree of concealment, carries small risk for the perpetrator, and is difficult to detect.
3) The perpetrators of Internet crime are often young people who hack into networks as a game.

4) Hackers usually do not commit this crime for economic benefits, although their actions may indirectly cause damage to the economy, endanger society, and even endanger national security.
5) Perpetrators usually target the networks of large financial and telecommunications companies, seeking to cause financial harm to the company out of malice or the desire for revenge.
6) The government has been relatively slow to monitor, control, and regulate Internet crime.

Although the People's Republic of China has already enacted laws to counter cybercrime, these are inadequate. China is in the process of drafting a new Internet Activity Law, but the legislators undertaking the revision must carefully craft laws that limit cybercrime without inhibiting lawful commercial activity and without infringing on the personal rights, privacy rights, and intellectual property rights of citizens and corporations.

DUTCH LITERATURE

Buruma, Ybo. "Acht nieuwe wetten: De zin en onzin van gegevensbescherming" [Eight new laws: The sense and nonsense in data protection]. *Delikt en delinkwent* [Offense and offender] 34, no. 7 (September 2004): 665–75.

Dutch law professor Ybo Buruma of the University of Nijmegen examines personal privacy in light of Dutch laws that allow government agencies to access citizens' financial, telecommunications, and other data in investigations of cybercrime and other offenses. Critics argue that these laws diminish personal privacy and permit authorities to treat individuals as criminal suspects based on random patterns that appear in their personal data, rather than on a prior basis for suspicion. However, Buruma argues that these laws have improved security, thereby justifying the moderate reduction in personal privacy that they entail. He also contends that Dutch law should not concern itself with whether or not authorities should have access to private data, but with how such access affects personal privacy. More specifically, Buruma suggests that an individual's free and independent determination of his or her life choices is an important dimension of privacy. Therefore, the law should require authorities to revise or delete erroneous data profiles of individuals so that those profiles do not limit individuals' private determination of life choices.

Buruma, Ybo. "De informatiemaatschappij en het strafrecht" [The information society and criminal justice]. *Delikt en delinkwent* [Offense and offender] 37, no. 6 (June 2007): 559–66.

University of Nijmegen law professor Ybo Buruma analyzes the effectiveness of Dutch criminal laws allowing authorities to examine citizens' financial and other data in the course of investigating cybercrime and other criminal offenses. Based on police data, the author contends that laws permitting this have not been effective in criminal investigations and prosecutions. Buruma also examines the effects of these laws on information security and on the privacy of those who have not committed any crime. Responding to critics of these laws, Buruma argues that authorities' power to examine citizens' data has not greatly threatened personal privacy, because these laws are of limited effectiveness and, consequently, their intrusiveness is limited.

In addition, he asserts that the laws do not threaten personal privacy, because their power is not as extensive as critics allege. In response to critics who argue that the government should adopt legal limits on authorities' use of personal data, Buruma contends that administrative and technological measures are a better means of protecting personal data than are legal measures. Just as speed bumps may force people to drive differently, even when legal speed limits fail to curb excessive speed, administrative and technological methods may prevent misuse of citizens' personal data even when laws fail to do so.

Buruma, Ybo. "Veiligheid en privacy" [Security and privacy]. *Delikt en delinkwent* [Offense and offender] 32, no. 4 (April 2002): 329–39.

The author, a law professor at the University of Nijmegen, addresses criticism of the Dutch security agencies' examination of Dutch citizens' financial, telecommunications, and other personal data in the course of criminal investigations. Buruma contends that, because the legal use of data collected during such investigations enhances the security of society, the collection of the data is justified. In addition, the author argues that critics often overlook various limitations that the legal system imposes on authorities' freedom to access and examine personal data. For example, he points out that Dutch courts require authorities to provide progressively greater justifications as they request increasingly extensive examinations of private data. However, Buruma also states that the government should provide additional safeguards when it permits authorities to access private data in their investigations. For example, he suggests that the government should more stringently screen officials who collect and analyze private information.

Grijpink, Jan H. A. M. "Een beoordelingsmodel voor de inzet van biometrie" [A critical model for the use of biometrics]. *Privacy en informatie* [Privacy and information] 9, no. 1 (February 2006): 14–17.

The author, a professor at the University of Utrecht, proposes methods for assessing potential problems with new and proposed security technologies, such as the use of biometric data in passports and other identity documents. Cautioning that authorities should consider the possibility of criminals misusing these security technologies, Grijpink proposes specific ways in which authorities can address potential problems that these technologies pose, thereby reducing the incidence of computer-related offenses and identity fraud. For example, the author suggests that authorities should change security procedures frequently to prevent potential offenders from anticipating and circumventing them.

Jacobs, Bart, and Wouter Teepe. "Over vermogen en onvermogen" [About ability and inability]. *Privacy en informatie* [Privacy and information] 10, no. 4 (August 2007): 142–46.

The authors, both professors of computer science at Dutch universities, examine controversies related to the Dutch government's use of information technology to collect and store individuals' personal data. Jacobs and Teepe discuss uses of information technology for elections and national security. They suggest that the Dutch government's use of information technology creates numerous opportunities for misuse of citizens' personal information. However, measures to prevent misuse of citizens' personal information could undermine effective data collection and processing.

Koops, Bert-Jaap, and Corien J. E. J. Prins. "Misbruik van technische hulpmiddelen: Een beschouwing over de te vergaande regelingen in het cybercrime-verdrag en de auteursrechtenrichtlijn" [Misuse of technology tools: A discussion of the far-reaching regulations in the cybercrime convention and the copyright directive]. *Computerrecht* [Computer law] 3 (2004): 59–67.

The article examines Dutch laws implemented to meet the requirements of the Council of Europe Convention on Cybercrime and its Copyright Directive (Directive 2001/29/EC). The authors argue that Dutch laws provide excessive punishments for minor cybercrime and copyright offenses, yet they do not sufficiently punish major offenses, such as hacking and data manipulation. Koops and Prins also provide several recommendations for Dutch domestic laws on cybercrime and copyright violations, such as better definitions of particular offenses and more sufficient punishments for major cybercrime and copyright offenses.

Koops, Bert-Jaap, Ronald E. Leenes, and Paul J. A. De Hert. "Grondrechten en nieuwe technologieën: Een rechtsvergelijkend overzicht" [Fundamental rights and new technologies: A comparative law overview]. *Nederlands juristenblad* [Dutch lawyers gazette] 83, no. 19 (May 9, 2008): 1157–64.

University of Tilburg professors Koops, Leenes, and De Hert summarize their research findings from a Dutch government-commissioned analysis of other countries' efforts to mitigate the harmful effects of information and communication technologies on citizens' individual rights, such as the right to privacy. They found that, although the use of information and communication technologies challenges fundamental individual rights, many countries have not modified their laws to prevent potential harm. Based on their findings, the authors recommend various changes to Dutch law aimed at protecting individuals from infringements related to information and communication technologies. Those recommendations include establishing constitutional protections for individuals' anonymity and for their stored data.

Leenes, Ronald E., Paul J. A. De Hert, Jos Vander Velpen, A. Thienpot, and Jonas Maebe. "Iedereen wordt er slechter van Europese regelgeving over het bewaren van gegevens bij misdaadbestrijding" [Everyone is worse off from the European Regulation on data retention in the fight against crime]. *Nederlands juristenblad* [Dutch lawyers gazette] 81, no. 24 (June 16, 2006): 1318–19.

The authors provide a critical analysis of a March 2006 Council of Europe directive on data retention (Directive 2006/24/EC). This directive is in the implementation phase as signatory states adopt domestic legislation incorporating its provisions. Because the Netherlands is a signatory state, Dutch jurists are currently evaluating legislation that will apply to Dutch citizens when their lawmakers incorporate the directive into Dutch law. The directive requires providers of communications networks and services—such as e-mail and mobile telephones—to save data on individuals' communications usage so that public authorities can access such data for use in detecting, investigating, and prosecuting serious crimes. Although EC officials contend that the measure is necessary to prevent terrorism, the authors suggest that the measure could lead to violations of citizens' privacy. The authors also express their concern that law enforcement

agencies might use the data to justify treating individuals as suspects even though they have no previous record of criminal activity.

Prins, Corien J. E. J. "Variaties op een thema: Van paspoort—naar identiteitsfraude" [Variations on a theme—From passport to identity fraud]. *Nederlands juristenblad* [Dutch lawyers gazette] 81, no. 1 (January 6, 2006): 9–14.

Dutch law professor Corien Prins examines vulnerabilities in government security measures designed to address computer-related crimes and identity fraud. The author argues that the use of biometrics, centralized information databases, and other security measures presents some problems, including high rates of error in identifying individuals and the use of these methods by criminals to perpetrate identity fraud and other crimes. The author cautions that politicians in the Netherlands and elsewhere often overemphasize the security and administrative efficiency benefits of these security measures while not paying sufficient attention to their related vulnerabilities. The article also provides several recommendations on how to avoid these problems when constructing security measures in the future.

The Netherlands. Ministry of Justice. *Justitiële verkenningen* [Judicial exploration] 30, no. 8 (2004).

This edition of *Justitiële verkenningen*—a serial published by the Ministry of Justice of the Netherlands—contains six articles on topics related to cybercrime. Some articles examine the effectiveness of Dutch laws and law enforcement agencies in policing cybercrime. The authors of these articles argue that Dutch authorities' power to undertake electronic surveillance and to access personal data when investigating cybercrime are insufficient for policing some types of computer-related crimes, such as computer-based attacks on public utilities and other public infrastructure. The authors recommend methods of improving cybercrime policing, including domestic measures and international cooperative efforts. Other articles in this volume discuss the effect of the Dutch government's electronic surveillance and data-access powers on Dutch citizens' civil liberties. These articles are generally critical in tone, and the authors suggest methods of protecting privacy and other civil liberties.

Van der Hulst, Reneé C., and Rudie J. M. Neve. "High-tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie" [High-tech crime, types of crime, and their perpetrators: A review of the literature]. Study, Boom Juridische Uitgevers, Wetenschappelijk Onderzoek en Documentatiecentrum, Ministry of Justice, The Hague, The Netherlands, 2008.

The Netherlands' Ministry of Justice commissioned this study, a literature survey of research on high-tech crimes and common characteristics of the perpetrators of those crimes. The analysis includes a list of the different types of high-tech crime, including the varieties of cybercrime, as well as an inventory of the characteristics of individuals and groups that perpetrate high-tech crimes. However, the authors caution that available publications provide little information on individual perpetrators of high-tech crimes.

Vedder, Anton, Leo van der Wees, and Bart-Jaap Koops. "Big Brother's bevoegheden zijn er—nu hij zelf nog?" [Big Brother's powers are still there—Is he?]. *Nederlands juristenblad* [Dutch lawyers gazette] 84, no. 41 (November 17, 2006): 2356–60.

University of Tilburg professors Vedder, van der Wees, and Koops discuss the increasing risks that technological developments pose to the privacy of citizens. Their analysis pays particular attention to the increase in the availability and accessibility of data, coupled with the augmented investigative powers of Dutch government agencies. The authors argue that the availability of individuals' personal data and government access to that data has diminished citizens' privacy and increased the risk of authorities treating a person as a suspect without probable cause. To remedy this risk, the authors recommend numerous measures, such as more input from the public regarding future computerization of private data and greater transparency in the government's investigative and judicial powers.

Vedder, Anton, Leo van der Wees, Bert-Jaap Koops, and Paul J. A. De Hert. *Van privacyparadijs tot Controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw* [From privacy paradise to control state? Fighting crime and terror in the Netherlands at the beginning of the 21st century]. Rathenau Instituut Study 49. The Hague: Rathenau Instituut, 2007.

The study examines the effect of the Dutch government's electronic surveillance measures on individual privacy in the Netherlands, discussing technologies that Dutch authorities use for the detection and prevention of crime and terrorism—technologies such as DNA profiling, surveillance cameras, wire-tapping, and, in particular, the use of digital databases. The study is generally quite critical of the methods of the Dutch government. The authors argue that the government's surveillance measures impinge on individual privacy and civil liberties without providing clear benefits for public safety and security.

FRENCH LITERATURE

Casile, Jean-François. *Le code pénal à l'épreuve de la délinquance informatique* [The challenge of cybercrime to the legal code]. Aix-en-Provence, France: Presses Universitaires d'Aix-Marseille, 2002.

The author, a law professor, provides a scholarly analysis of French laws on cybercrime. The first part of the book provides a justification for changing the French legal code with respect to automated data processing and telecommunications. The second part proposes a methodology for approaching legal reform in this area.

Cédras, Jean. "Un aspect de la cybercriminalité en droit français: Le téléchargement illicite d'œuvres protégées par le droit d'auteur" [An aspect of cybercrime in French law: The illicit downloading of works protected by intellectual property rights]. *Revue internationale de droit pénal* [International review of penal law] 77, no. 3–4 (2006): 589–610.

The volume of illicit downloads on the Internet poses a threat to the industries of arts and culture, because it infringes upon the rights of authors. This article analyzes the treatment under French law of the illicit downloading of works protected by intellectual property rights. Specifically, it explains the responsibility of various participants, such as the Internet user or the access provider, as well as offering possible justifications for downloading, such as exceptions for making copies for private use.

Debray, Stéphane. "Internet face aux substances illicites: Complice de la cybercriminalité ou outil de prévention?" [The Internet confronts illicit substances: Is it complicit in cybercrime or a tool for prevention?]. Report, Droit et Nouvelle Technologies [Law and New Technologies], Brussels, January 28, 2004. http://www.droit-technologie.org/upload/dossier/doc/134-1.pdf.

This report focuses on an aspect of cybercrime that has not attracted much attention, even though it is extremely dangerous: trafficking in soft, hard, and performance-enhancing drugs and pharmaceuticals. In the first part of the report, the author discusses ways the Internet can promote illegal activity and the commercialization of harmful drugs and pharmaceuticals. The second part of the report involves the opposite perspective: specifically, how the Internet can serve as a beneficial tool for prevention and research in the areas of health and toxicology. The third part of the report proposes defensive measures and legislation the government could enact to combat cybercrime.

Esterle, Alain. "Le développement des TIC à l'épreuve de la sécurité" [The development of information and communication technology (ICT) as a test of security]. *Réalités industrielles* [Industrial realities], November 2005, 62–67.

According to the author, analysts increasingly agree that security of information and networks is necessary for the development of information and communication technology. European countries are moving in a more coherent and complementary direction with respect to information security. The development of an industrially and operationally competitive technology base at the national and European level is the new goal. The author, an information security executive, finds that information security (also known as Infosec) concerns three actors: the citizen, the enterprise (company), and the responsible state authorities. He elaborates the French and European perspectives of the three phases of Infosec—protecting information systems, preventing incidents, and responding to them (including the imposition of penalties).

Ferchaud, Bernadette. "Journée d'étude SCIP France: L'intelligence économique face aux défis des nouvelles menaces" [One-day conference sponsored by SCIP France: Economic intelligence faces challenge from new threats]. *Documentaliste—Sciences de l'information* [Document librarian—Information science] 39, no. 4–5 (2002): 228–31.

In this article, the author reports the activities of a conference, which occurred in June 2002, on new threats to economic intelligence. The French Society of Competitive Intelligence Professionals sponsored the conference. Participants identified cybercrime aimed at the illegal acquisition of privileged economic data as an emerging threat facing government agencies, businesses, and individuals (listed in order of how acute the threat is to this type of entity). The profile of perpetrators is as follows: 49 percent are employees of the targeted company, 41 percent are independent of any organization, and the rest work for competing firms, government agencies, or foreign governments. The article also enumerates key vulnerabilities of victims of crimes and discusses the motivations of the perpetrators.

Iteanu, Olivier. *Tous cybercriminels: La fin d'Internet* [All are cybercriminals: The end of the Internet]. Paris: Jacques-Marie Laffonts Editeurs, 2004.

The book begins with a definition and general discussion of cybercrime and then provides 14 case studies, which include examples of actual instances of identity theft, spamming, e-mail bombing, data sabotage, and software theft. In the second part of the book, the author discusses the implications of cybercrime for the victim, the perpetrator, oversight authorities (the government, the police, etc.), and for the Internet itself. The author also explains how institutions can use legal and technical means to defend themselves.

Martin, Daniel, and Frédéric-Paul Martin. *Cybercrime: Menaces, vulnérabilités et ripostes* [Cybercrime: Threats, vulnerabilities, and countermeasures]. Paris: Presses Universitaires de France, 2001.

Daniel Martin is the director of the French National Police and a security official at the Organisation for Economic Co-operation and Development (OECD). Frédéric-Paul Martin is an attorney and legal consultant specializing in new information and communication technologies. Both are founders of the Paris-based Cybercriminstitut. The first part of the book has separate sections on laws relevant to cybercrime; threats to individuals, companies, and the government; profiles of various types of cybercriminals, ranging from hackers to company insiders; and the motivations of cybercriminals. The second part of the book outlines the response to cybercrime at the national (French), European, and international levels. The third part focuses on the future and on potential opportunities for stemming cybercrime.

"Menaces informatiques et pratiques de sécurité en France" [Security practices and threats to data in France]. Report, Club de la Sécurité de l'Information Français (CLUSIF) [French Information Security Club], Paris, 2008. http://www.clusif.asso.fr/fr/production/sinistralite/docs/CLUSIF-rapport-2008.pdf.

In January 2009, the French Information Security Club published its eighth annual overview of cybercrime in France, covering the events of 2008. This 84-page document presents the results of

a survey of 354 French businesses with more than 200 employees; 194 towns and cities with more than 30,000 inhabitants; and 1,139 individuals. The report addresses specific issues delineated in the ISO/IEC 27002 Code of Practice for Information Security Management: security policy; organization of information security; asset management; human resources security; physical and environmental security; communications and operations management; access control; information systems acquisition, development, and maintenance; information security incident management; business continuity management; and compliance.

Padova, Yann. "Un aperçu de la lutte contre la cybercriminalité en France" [An overview of the battle against cybercrime in France]. *Revue de science criminelle et de droit pénal comparé* [Review of comparative criminal science and penal law], no. 4 (October–December 2002): 765–80.

In this article, Yann Padova, an official assigned to the French National Assembly, maintains that French laws are inadequate for dealing with cybercrime. He states that the French police do not have suitable instruments at their disposal for combating the threat. In addition, he describes numerous jurisdictional conflicts—including those at the international level—that hinder authorities from addressing the cybercrime threat. However, the author adds that the Council of Europe is considering some initiatives that could ameliorate the situation.

Quéméner, Myriam. "Cybercriminalité: Aspects stratégiques et juridiques" [Cybercrime: Strategic and legal aspects]. *Défense nationale et sécurité collective* [National defense and collective security], no. 5 (May 2008). http://www.droitalenfance.com/download/Quemener[1].pdf.

This article focuses on French and European Union laws targeting cybercrime and suggests how authorities can make better use of them. The author explores the new challenges that Internet and local digital networks pose to people who depend on these networks for their economic livelihoods, explaining the need to defend the networks against cybercrime. Quéméner defines cybercrime as criminal activities conducted by means of Internet technology in cyberspace. Digital networks are spawning new violations of social and individual rights, necessitating the constant adjustment of the governmental, legislative, police, and judicial response. Information and communication technologies are apparently an ideal medium for promoting a wide variety of criminal activities. The author distinguishes two types of cybercrime: 1) crimes involving the unauthorized access to data and systems for criminal purposes; and 2) crimes involving fraud, falsification, the diversion of funds, obtaining illicit content, or defamation via online services. New technologies are both a target and a medium for new forms of criminality, such as hacking, cracking, and *phreaking*—cracking a telephone network to make free, long-distance calls.

Vitaline, Vanessa. "Cybercriminalité—Délinquance financière différentes escroqueries liées aux réseaux informatiques" [Cybercrime—Various forms of financial fraud related to data networks]. Master's Thesis, Université Paul Cézanne d'Aix-Marseille, France, October 2006.

In this 196-page master's thesis, the author discusses the common threat of cybercrime to all parts of society. Certain threats concern everyone, such as *keylogging*—using software or

devices to secretly monitor and record keystrokes, enabling espionage activities or the harvesting of personal data. Others, such as denial-of-service (DoS) attacks, target companies and governments, inundating their networks with tasks that occupy the computer system's resources and render it unavailable to authorized users. Cybercriminals aim to seize data of commercial value, to steal passwords, and to use cryptography to carry out their fraudulent activities. These offenses involve acts of destruction when the purpose is to deprive a company of its institutional memory. Criminals are invading cyberspace, attracted by the possibility of fast profit. The author identifies several characteristics typical of this criminal activity: cybercrime is low cost, high speed, and anonymous; it has a global impact; and its perpetrators use remote intervention to carry out their crimes with impunity. Cybercriminals recruit experts in data processing and networking to assist them in using an arsenal of increasingly powerful tools, such as the *rootkit*—software permitting covert takeover of a targeted computer system. The author describes the modus operandi of the cybercriminal, explaining how cybercrime operates as a business and what participants have at stake. Governments and police authorities have taken certain countermeasures that some decry as imposing restrictions on personal freedom. Nevertheless, cybercrime continues to grow exponentially, and criminal organizations continue to benefit.

GERMAN LITERATURE

Kempa, Darius. "Angriff auf Netze und Systeme: Hackerkultur zwischen gesellschaftlicher Anerkennung und Kriminalisierung" [Attack on Networks and Systems: Hacker Culture between Social Recognition and Criminalization]. Dissertation, University of Hamburg, Germany, August 9, 2006. http://www.sub.uni-hamburg.de/ opus/volltexte/2006/3025/ index.html.

In this dissertation, completed at the University of Hamburg, Darius Kemper attempts to define computer crime, placing in a criminological context all known cybercrimes to date. The first part of this three-part work creates an overview and typology of existing computer crimes, emphasizing those committed by hackers. Kemper discusses types of offenses that perpetrators have committed; the special characteristics of these crimes; the new forms of crime that have emerged with the widespread use of computers; and how to categorize these offenses. In the second part, the author uses secondary literature, attempting to analyze and understand the new criminal groups that have emerged. Observers often characterize hackers as the main actors in cybercrime. This dissertation addresses the structure of the hacker milieu. In the third part of the dissertation, the author explores the underlying motivation driving hacker behavior from a criminological perspective, referring to self-control theory.

Köppen, Hajo. "Entwicklung der Computerkriminalität in den Jahren 2004 bis 2007" [Development of Computer Crime in the Years 2004 to 2007]. *Datenschutz und Datensicherheit* [Data Protection and Data Security], December 2008. http://www.dud.de.

Since 1953, the German Ministry of the Interior has published annual police criminal statistics. However, these statistics only include crimes registered by the police, and, therefore, they do not provide an accurate mirror of cybercrime. Rather, the statistics provide an approximation that

reflects the reality of computer crime more or less, depending on the nature of the infraction. Because the laws addressing computer crime are more than 20 years old, the data on this type of crime contains significant gaps. However, this presentation of the police statistics for 2004–2007 remains useful.

Poller, A. "Privatsphärenschutz in Soziale-Netzwerke-Plattformen" [Privacy Protection in Social Network Platforms]. Study, Frauenhofer Institut für Sichere Informationstechnologie [Frauenhofer Institute for Secure Information Technology], Darmstadt, Germany, September 23, 2008. http://publica.fraunhofer.de/eprints/urn:nbn:de:0011-n-818929.pdf.

This study analyzes the mechanisms that seven social-networking platforms use for protecting private data—Myspace, facebook, studiVZ, wer-kennt-wen [who knows whom], lokalisten, X ING, and LinkedIn. Social-networking platforms are Internet-based applications in which the users model their relationships to other people, using this information for important service functions. The processed data are usually of a personal nature. If weak spots exist in the social-networking site's security or if the site lacks protective measures, the potential danger for users is correspondingly high. Legal analysts view social-networking platforms as a potential target of cybercrime. This study evaluates the security and protective measures of popular social-networking platforms from the perspective of a regular Internet user.

Sokol, Bettina. "Achtzehnter Datenschutz- und Informationsfreiheitsbericht" [Eighteenth Data Protection and Information Freedom Report]. Report, Landesbeauftragter für Datenschutz und Informationsfreiheit [State Representative for Data Protection and Information Freedom], North Rhine-Westphalia, Germany, 2006. https://www.ldi.nrw.de/mainmenu_Service/submenu_Berichte/index.php.

The Representative for Data Protection and Information Freedom of the German state of North Rhine-Westphalia publishes a status report every two years. The 18th annual report, which covers 2005 and 2006, contains sections on technology, media, video surveillance, employment data protection, official data protection, international data traffic, information freedom, the police, the judiciary, municipal enterprise, the activities of the German Office for the Protection of the Constitution, the economy, finances, education, science, social affairs, health, and the 2006 soccer world championship.

Vetter, Jan. "Gesetzeslücken bei der Internetkriminalität" [Gaps in the Law regarding Internet Crime]. Dissertation, University of Konstanz, Germany, November 11, 2002. http://www.ub.uni-konstanz.de/kops/volltexte/2002/927/pdf/diss_vetter.pdf.

The dissertation identifies gaps in the law regarding Internet crime. The author Jan Vetter reviews relevant German laws and, to some extent, the laws of other countries, such as Switzerland and France, identifying areas in which the rapidly evolving techniques used in Internet crime have outpaced static legal prohibitions. Vetter focuses specifically on the installation of distributed denial-of-service (DDoS) agent programs—programs that use numerous infiltrated computer systems to attack a network from many directions, flooding the target system's resources so that DDoS results—and the offering of computer virus construction

kits via the Internet. After explaining the technology of the Internet, Vetter explores its social significance and reports selected relevant criminal statistics.

In the second part of the thesis, he examines the development of legislation regarding computer crimes, including a detailed presentation of German criminal law pertaining to business and to information and communication services. The third part of the thesis analyzes existing law in the area of Internet crime, identifying possible loopholes in law. In the fourth part, Vetter discusses the necessity of providing for Internet crime within the field of criminal law, specifically, suggesting possible reforms to close the loopholes in existing law. Finally, the author briefly describes the Convention on Cybercrime for fighting computer and Internet criminality, an agreement that several member countries of the Council of Europe signed in Budapest on November 23, 2001.

In conclusion, the author observes that German laws have not kept pace with the many different and continually evolving forms of Internet crime. For example, Germany needs to enact legislation specifically criminalizing the massive spreading of computer viruses. However, Vetter also points out that the legal solution alone is inadequate, recommending the necessity of additional measures, both legal and technical, to prevent Internet crime. Because the author discovered during his research that very little secondary literature existed on his topic, he believes that his dissertation has explored new ground.

ITALIAN LITERATURE

Antinori, Arije. "Information Communication Technology and Crime: The Future of Criminology." [In English.] *Rivista di Criminolgia, Vittimologia e Sicurezza* [Journal of Criminology, Victimology, and Security] 2, no. 3 (September–December 2008): 23–31. http://www.vittimologia.it/rivista/articolo_ antinori_2008-03.pdf.

Antinori considers the global, Internet-based economy a key factor in social change and suggests that cyberspace hosts new models of social deviance. Furthermore, because traditional terrorist groups are also using this new media, the author recommends that governments pay special attention to the phenomenon of cyberterrorism—also known as "digital jihad," "infowar," "netwar," and "mediawar." Criminologists must understand the role of digital culture in crime and must acquire the necessary skill in information and communication technologies to prevent and counteract such crimes and to envisage future cybercrime trends.

Apruzzese, Antonio. "Dal computer crime al computer-related crime" [From computer crime to computer-related crime]. *Rivista di Criminolgia, Vittimologia e Sicurezza* [Journal of Criminology, Victimology, and Security] 1, no. 1 (January–April 2007): 55–60. http://www.vittimologia.it/rivista/apruzzese%202007-01-01.pdf.

Digital identity theft, also known as *phishing*—illegally accessing an individual's financial data to capture online banking and financial information—has become one of the most lucrative illegal businesses. When this type of criminal activity first began, perpetrators victimized individuals, but now, criminals tend to attack computer networks. Some of the latest and most sophisticated data-processing techniques that these cybercriminals use are *pharming* (directing

traffic from a legitimate Web site to a site controlled by a criminal hacker), *keylogging* (monitoring and recording keystrokes), and, most recently, *botnets*—networks of infected machines, usually managed by a single command center, and capable of causing serious damage to networked systems. Organized crime syndicates are increasingly using botnets, which have made large-scale identity theft much simpler to realize. To respond more effectively to this rising challenge, the Italian State Police has created the Servizio Polizia Postale e delle Comunicazioni (Postal and Communication Police), a new agency that specializes in combating this type of crime.

Carlesi, Carlo. "Sicurezza informatica and 'computer crime'" [Computer security and 'computer crime']. Report, Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo [Alessandro Faedo Institute of Computer Science and Technology], Pisa, 2003. http://74.125.47.132/search?q=cache:5N2P81etagQJ:its.isti.cnr.it/CarloDoc/SICC.pdf+http://its.isti.cnr.it/CarloDoc/SICC.pdf&cd=1&hl=en&ct=clnk&gl=us.

Carlo Carlesi reports on computer crime, which became a serious problem in the 1990s with the enormous growth of the Internet. He divides computer crime into two broad categories: crimes committed using a computer—most notably, pedophiles' use of the Internet for child pornography and to victimize children—and crimes targeting computer files, such as the illicit use, theft, or manipulation of data. Italy was among the first European countries to pass legislation to protect computer data and to create a government entity (the Authority for Information Technology in the Public Administration—AIPA) to take responsibility for the protection of data. Carlesi lists several types of attack against computer systems: unauthorized access, service interruption, introduction of viruses, interception of transmissions, and creation of false identities.

Pomante, Gianluca. "Hacker! Criminali o eroi della rivoluzione informatica" [Hackers! Criminals or heroes of the computer revolution]. Presentation at the conference on Information, Technology, and Law, University of Urbino, Italy, November 20, 2000. Accessed via the Web site *Hacker Kulture*. http://www.dvara.net/HK/pomante.asp#top.

In this eight-page article, Gianluca Pomante, the author of several books about computer crimes, outlines the origins of hacking, which began at Massachusetts Institute of Technology (MIT) in the late 1950s, explaining how hacking developed and how it became a tool of cybercriminals. Pomante presents a graphic by Ira Winkler that divides hackers into three categories: geniuses, tool developers, and ordinary skilled users of the Web. The graphic indicates that criminals and foreign intelligence agencies may possess characteristics that place them within any of the three categories. Whether hacker geniuses, tool developers, or ordinary skilled users, criminals and foreign intelligence agencies use the tools and knowledge they have to gain information about their targets. Although Pomante concedes that hackers are capable of using their skills to commit serious crimes and to cause damage via the Web, he warns that legislation against these activities could harm future creative development of the Web, if the laws against hacking do not distinguish between the occasional transgressions of hackers and criminal activities that harm others.

Rosini, Luciano. "Il computer crime e le strategie di constrasto" [Computer crime and contrasting strategies]. *Revista di Criminolgia, Vittimologia e Sicurezza* [Journal of Criminology, Victimology, and Security] 1, no. 1 (January–April 2007): 12–17. http://www.vittimologia.it/rivista/rosini%202007-01-01.pdf.

The development of the Internet has opened opportunities of growth in many sectors, redefining daily life, but it has also engendered new forms of cyberspace criminality that challenge legal systems and traditional investigative procedures. Moreover, national boundaries do not confine cybercrime, which is transnational. In 1998, to cope with the dangers and risks of cybercrime, Italy established the Servizio Polizia Postale e delle Comunicazioni (Postal and Communication Police), with the aim of conforming Italy's investigative procedures to international standards and of responding to the threats posed by this technological and cultural transformation.

Stilo, Leo. "Il crimine informatica in azienda" [Computer crime in a business]. *Computerlaw informatica e diritto* [Computer science and law], March 17, 2007. http://www.computerlaw.it/entry.asp?ENTRY_ID=256.

Leo Stilo's article about a January 2006 IBM study of computer crimes in businesses appeared in the online journal *Computerlaw informatica e diritto*, which publishes articles, information, and commentary about many aspects of law relating to computers. According to Stilo, the IBM study found that 23 percent of Italian executives regard computer crime as more dangerous than traditional crime, while 40 percent regard it as of equal danger. In addition, 46 percent of Italian executives believe that computer crime is more damaging financially than traditional crime, and 51 percent think that the threat to a business from within the company is greater than the threat from external sources. Stilo also cites a specialist who contends that hackers are not the real threat to companies but that computer crimes mostly originate inside businesses.

Vulpiani, Domenico. "La nuova criminalita informatica. Evoluzione del fenomeno e strategie di contrasto" [New computer criminality: Evolution of the phenomenon and strategies to combat it]. *Rivista di Criminologia, Vittimologia e Sicurezza* [Journal of Criminology, Victimology, and Security] 1, no. 1 (January–April 2007): 46–54. http://www.vittimologia.it/rivista/vulpiani%202007-01-01.pdf.

The shared knowledge of the Internet requires us to harmonize technological growth with security policies that protect both the technological infrastructure and individuals. Therefore, the Italian Servizio Polizia Postale e delle Comunicazioni (Postal and Communication Police) has recently introduced innovations to combat the risk of computer crimes and computer-related crimes, including the establishment of the Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche Informatizzate (National Center Against Information Crime for the Protection of the Critical Information Infrastructure); the Child Exploitation Tracking System, to fight online pedophilia; and the first online police station, the Online Police Office for Security (OLPS).

JAPANESE LITERATURE

Ibusuki, Makoto. "Saibā hanzai wo meguru tetsuzuki ho teki syomondai" [Issues on the legal procedures surrounding cybercrimes]. Paper presented at the 84th conference of the Japanese Criminal Law Society. *Keihō zasshi* [Japanese criminal law journal] 46, no. 2 (February 2007): 290–93.

This paper summarizes various legal issues presented at this workshop, held at the 84th Conference of the Japanese Criminal Law Society. The society held the workshop to discuss the Council of Europe Convention on Cybercrime, which Japan, the United States, and four other non–European Union countries signed in November 2001 at the European Union Summit.

Ibusuki, Makoto. "Saibā hanzai jyōyaku oyobi sono kokunaihouka ni tsuite" [On domestic legislation following the Convention on Cybercrime]. In "Tokusyū-Saibā keijihou no doukou to kadai" [Special issue: Trends and issues regarding criminal law on cybercrime]. *Keihō zasshi* [Japanese criminal law journal] 45, no. 1 (July 2005): 118–29.

In November 2001, Japan signed the Council of Europe Convention on Cybercrime, and in April 2004 the Japanese parliament approved Japan's participation in the Convention. During the implementation phase, signatory countries, including Japan, are implementing domestic legislation to enact the Convention's directive for their own citizens. The author discusses the Japanese parliament's preparation of new legislation on cybercrime. Ibusuki lists relevant details of each new criminal law.

Katō, Yō. "Saibā hanzai ni kansuru jyouyaku" [The Convention on Cybercrime]. In "Tokusyū: Dai 159kai kokkai syuyō seiritsu houritsu" [Special issue: Major legislation of the 159th Parliament]. *Jurisuto* [Jurist], September 1, 2004, 81–83.

This article summarizes in detail the Convention on Cybercrime signed in Budapest, Hungary, in 2001 (an international collaboration on criminal law regarding cybercrime), as well as the process of the new legislation discussed during the 159th Diet in Japan.

Kawaishi, Isamu. "Saibā hanzai no genjyou nado ni tsuite" [Current issues on cybercrime, etc.]. *IEICE technical report* 108, Institute of Electronics Information and Communications Engineers, Tokyo, July 18, 2008, 17–20.

This Powerpoint presentation introduces statistics on the increase in the number of cybercrimes, as well as on arrests related to cybercrime in Japan for the last five years. In addition, the presentation provides examples of the most common cybercrimes in Japan, including information security (leaks of personal information) through phishing; exploitation through social sites; computer gambling; child pornography; marketing illegal items, such as drugs, over the Internet; and copyright violation. The speaker also explains how cybercrimes are committed, including cases in which cybercriminals attack computers not connected to the Internet.

Keisatsu Seisaku Gakkai, Keisatsu Seisaku Kenkyu Sentā [Police Policy Society, Police Policy Center]. "Saibā hanzai: Keisatsu seisaku forum saibā hanzai boushi taisaku" [Cybercrime: Police Policy Forum on measures for the prevention of cybercrime]. *Keisatsugaku ron syū* [Papers on police studies] 60, no. 1 (January 2007): 122–59.

The Japanese National Police Center invited experts from the United States and the United Kingdom, who are currently leading their national security branches for cybercrime, to help Japan understand and manage the burden of cybercrime. This article introduces the forum.

Livesley, Andrew, and Kōichi Kurokawa. "Jyudai soshikihannzai taisaku cho no setsuritsu to saibā hanzai taisaku" [The Ministry for the Prevention of Large-Scale Organized Crime and measures for the prevention of cybercrime]. In "Keisatsu seisaku forum saibā hanzai/saibā tero taisaku no suishin ni mukete" [Police Policy Forum: Measures for the prevention of cybercrime/cyberterrorism]. *Keisatsugaku ron syū* [Papers on police studies] 60, no. 1 (January 2007): 136–51.

The author explains in detail the cybercrime-related activities of Japan's SOCA (Serious Organized Crime Agency). The electronic/cybercrimes prevention team reports to one of the four branches of SOCA Intervention. This branch of SOCA Intervention includes five different groups: Crime Benefit, Electronic Crimes, International, Crime Technology, and Prevention. The groups collaborate with one another on many of their activities.

Matsui, Shigenori. "Kokkyou no anzen to intānetto jyou no jinken" [Public safety and human rights on the Internet]. In "Tokusyu-anzen to shiteki jichi, tetsuzukiteki seigi dai 29 kai hou to konpyūta gakkai kenkyukai houkoku" [Special issue: Safety, autonomy, and justice. Report presented at the 29th annual meeting of the Society for Law and Computing]. *Hou to konputā* [Law and computers] 23 (July 2005): 3–17.

The author argues that, since September 11, people throughout the world have become more willing to relinquish privacy in exchange for the hope of safety. In this article, the author carefully examines whether, even if laws restricting freedom of expression make it easier to prosecute cybercriminals, these laws actually promote cyber security.

Natsui, Takato, Atsushi Yamaguchi, and Tadashi Sakamaki. "Soukatsu intanetto no riyou to kisei—dai 27kai hou to konppyutā gakkai kenkyu kai paneru disukasshon saibā hanzai jyouyaku to kokunai hou no taiou" [Summary: Usage and regulation of the Internet—27th Law and Computing Seminar Panel discussion on the Convention on Cybercrime and domestic measures]. In "Tokusyū: Intanetto no riyou to kisei" [Special issue: Usage and regulation of the Internet]. *Hou to konputā* [Law and computers] 21 (July 2003): 101–106.

Takato Natsui, chair of the panel discussion on the Convention on Cybercrime, summarizes basic rules and key points for discussion, listing the topics of illegal access to stand-alone computers, management of illegal interceptions, management of illegal programs, separation of data regarding traffic from content data, the possibilities of intercepting binary data, the use of current

law on communication interception, and the responsibilities of providers to collaborate with police.

Okada, Yoshifumi. "Saibā hanzai" [Cybercrime]. In "Tokusyū: Chian houkai" [Special issue: The destruction of public order]. *Gyros* [Current issues] 12 (March 2005): 94–102.

This article discusses the types of cybercrime that Japan should address pursuant to its 2001 signing of the Council of Europe Convention on Cybercrime and names three methods of combating cybercrime: advances in technologies, education of users, and establishment of advanced legal systems. The author considers methods that law enforcement agencies can use to detect a cybercrime as soon as possible after the commission of the crime.

Sakamaki, Tadashi. "Saibā hanzai jyouyaku no tetsuzukihou kitei ni tsuite" [On establishing the procedure: Act and provisions of the Convention on Cybercrime]. In "Tokusyū: Internetto no riyou to kisei—dai27 kai hou to konpyuta gakkai kenkyukai houkoku" [Special issue: Usage and regulation of the Internet—27th Law and Computing Seminar]. *Hou to konputa* [Law and computers] 21 (July 2003): 57–64.

The author explains how Japan has revised its criminal laws since signing the Council of Europe Convention on Cybercrime. In establishing new criminal laws, Japanese legislators found that the key issues included requests for communication records, requests to provide data regarding a suspected crime, confiscation of media for recording and investigating, and general requests for criminals to cooperate in investigations.

Sakuma, Osamu. " Jyouhou hanzai/Saibā hanzai" [Information crime and cybercrime]. In "Toksyū: Keihouten no hyakunen–rippō no kadai" [Special issue: 100 years of the penal code—Issues of legislation]. *Jurisuto* [Jurist], January 1, 2008, 108–16.

The author emphasizes the importance of Japan's laws dealing with cybercrime. Until now, the Japanese government has only established local ordinances, rather than statutory law, to deal with each cybercrime case. The author compares the legal system of Japan with that of Germany, proposing that Japan could learn more about the laws of both countries. In the future, Japan should carefully consider which cybercrimes to include in its law.

Sakuma, Osamu. "Saibā hanzai taisaku—Tamino doryoku wo ato oshi surumono" [Measures for the prevention of cybercrime—Efforts in support of the prevention of cybercrime]. In "Keisatsu seisaku fōramu saibā hanzai/saibā tero taisaku no suishin ni mukete" [Police Policy Forum on Cybercrime—Measures for the prevention of cyberterrorism]. *Keisatsu seisaku kenkyu* [Police policy research] 11 (2007): 93–97.

The author discusses the importance of collaboration between the government and the public in the fight against cybercrime and outlines the difficulties in doing so. At the beginning of 2007, the Japanese National Police Agency established an Internet hotline to investigate cybercrime. The author argues that, although Internet providers have been willing to collaborate with the government to stop cybercrime, they have had difficulty doing so, because privacy laws in Japan, aimed at protecting users, often protect those who are committing cybercrimes.

Satō, Takashi. "Kokkyou wo koeru saibā hanzai ni taisuru 'kokusai kyoudou sousa' ni tsuite-kousatsu" [Considering the international investigation of cybercrimes around the world]. *Keisatsugaku ron syū* [Papers on police studies] 58, no. 11 (November 2005): 156–80.

In this article, the author provides a clear definition of cybercrime, explaining how different cybercrimes compare to traditional crimes and how international collaboration and early detection are crucial in bringing criminals to justice.

Sung, Kijung, Naomichi Suzuki, Masatoshi Tanaka, and Kazuhiro Kasai. "A study of the meanings and techniques of cybercrime in advanced information society." [In English.] *Journal of Matsumoto University* 6 (January 1, 2008): 63–83.

This article discusses the historical background of cybercrime and the definition of cybercrime, contrasting cybercrime to information crime. Computer crimes are included in cybercrimes.

Takinami, Hirofumi. "Saibā hanzai ni kansuru jyouyaku' ni tsuite" [On the Convention on Cybercrime: Its meaning for the regulation of criminal justice]. *Keisatsugaku ron syū* [Papers on police studies] 55, no. 5 (May 2002): 124–45.

In this detailed summary, the author comments on the Council of Europe Convention on Cybercrime, discussing the meaning of the treaty and the process of its establishment.

Takinami, Hirofumi. "Saibā hanzai ni kansuru jyouyaku' ni tsuite tetsuzuki hou oyobi kokusai kyouryoku kitei" [On the Convention on Cybercrime: The law of procedure and provisions for international collaboration]. *Keisatsugaku ron syū* [Papers on police studies] 55, no. 9 (September 2002): 150–73.

The author summarizes an international treaty that Japan signed—the Council of Europe's Convention on Cybercrime. This treaty includes an introduction, followed by sections on criminal substantive law, procedure, territorial rights, international collaborations, and final acts.

Takinami, Hirofumi. "Saibā hanzai ni kansuru jyouyaku' ni tsuite tetsuzuki hou oyobi kokusai kyouryoku kitei" [On the Convention on Cybercrime: The law of procedure and provisions for international collaboration]. *Keisatsugaku ron syū* [Papers on police studies] 55, no. 10 (October 2002): 113–37.

The article summarizes procedural law on cybercrime, focusing specifically on the Act 14-21 regarding real-time samplings of computer data.

Watanabe, Akira. "Saibā hanzai no genjyō to taisaku" [Current issues and measures on cybercrimes]. In "Chushin tēma: Netto shakai no mondai wo kangaeru" [Main theme: Pondering issues of Internet societies]. *Kosei hogo* [Parole] 59, 4 (April 2008): 6–10.

The author provides examples of cybercrime cases, which have increased in recent years. The types of cases include 1) obtaining illegal access to someone else's computer for the purpose of illegal drug dealing; 2) manipulation of electronic money-transfer sites for the purpose of

stealing money; 3) the illegal distribution of copyrighted materials using file-share software; and 4) crimes common among teenagers, such as spending money on online games using someone else's passwords or teenage prostitution via online dating sites. Watanabe encourages the use of filtering systems and of counseling systems that the police have provided.

Yamada, Toshiyuki. "Wagakuni ni okeru saibā hanzai taisaku—Ousyuhyougikai saibā hanzai ni kansuru jyouyaku to kanren ni oite" [Measure against cybercrime in our country: A summary of the Convention on Cybercrime]. *Houritsu no hiroba* [Plaza of law] 57, no. 7 (July 2004): 47–50.

The author summarizes the key points of the Convention on Cybercrime, considering both substantive and procedural aspects of criminal law.

Yamaguchi, Atsushi. "Saibā hanzai ni taisuru jittaihouteki taiou" [Measure against cybercrime using substantive law]. In "Tokusyū: Haiteku hanzai ni taisuru rippo kodai" [Special issue: Legislaive challenges on high-technology crime]. *Jurisuto* [Jurist], December 1, 2003, 15–21.

The author addresses issues discussed during the Council of Europe Convention on Cybercrime. Yamaguchi lists key offenses, explaining each one, including illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offenses related to child pornography, and offenses related to infringement of copyright and related rights.

Yamaguchi, Atsushi. "Saibā hanzai jyōyaku no jittaihōteki igi" [The meaning of the substantive law of the Convention on Cybercrime]. In "Tokusyū: Intanetto no riyou to kisei—Dai 27 kai hou to konpyuta gakkai kenkyukai houkoku" [Special issue: Usage and regulation of the Internet—The 27th Law and Computing Seminar]. *Hou to konputa* {Law and computers] 21 (July 2003): 51–55.

In this article, the author explains what the Council of Europe expects of Japan after signing the Convention on Cybercrime and describes the type of laws Japan needs to establish to match these expectations.

Yamashita, Yukio. "Saibā hanzai jyouyaku' ga nihon no sosakatsudo wo kakudaisuru—Tokusyu-Jyouhouka shakai wa kokomade kiteiru" [The Convention on Cybercrime helps expand the investigation of cybercrime activities in Japan]. *Chūō kōron* [Center for public opinion] 117, no. 10 (October 2002): 152–57.

In this article criticizing the Council of Europe Convention on Cybercrime, which the Japanese government signed, the author covers a number of issues. First, the author argues that the Japanese police force is not familiar with the "real time" investigation of cybercrimes; the police do not understand that they have to investigate a crime as soon as it occurs, or even before hand. The author doubts that the Japanese police force is ready for this new approach. Second, the author explains that cybercrimes are often international crimes. According to the international treaty Japan has signed, if a foreign country requests access to cyber communications (including

text messages), the Japanese government must provide the information. The author suspects that, in some cases, Japan could receive a request that is not genuine. As an example, the author cites the case of the Echelon international taping system. The author is concerned that a foreign country might request the information to benefit themselves in some way other than the control of cybercrime. The author doubts that the Japanese government is sufficiently aware of the possible consequences of their obligations to other countries.

Yoshida, Kazuhiko. "Kojin jyouhou no fusei torihiki nado ni kakawaru saibā hanzai nado no genjyou to taisaku ni tsuite" [Current issues and measures for prevention of illegal exchange of personal information]. *Keisatsugaku ron syū* [Papers on police studies] 58, no. 11 (November 2005): 132–55.

In recent years, the increase in the occurrence of cybercrime has heightened the public's awareness of the importance of securing personal information. In this article, the author discusses two main crimes involving personal information: 1) the act of obtaining personal information illegally and 2) the act of using personal information for crimes.

KOREAN LITERATURE

Korean Language Sources (Republic of Korea—South Korea)[1]

Kim, Yŏn-su. *Saibŏ pŏmjoe ch'ongnam: Sinjong pŏmjoe (k'ŏmp'yut'ŏ pŏmjoe) sakŏn ŭi baibŭl* [Overview of cybercrime: The Bible for cases of a new kind of crime (computer crime)]. Seoul: Pŏmnyul Midiŏ [Legal Media], 2003.

This 1,492-page book discusses cybercrime in general, focusing on how cybercrime affects individual users, rather than government or commercial users, and emphasizing the protection of personal information. The author, Kim Yŏn-su (variants Kim Yon-su and Kim Yeon-su), is an information technology columnist working for AhnLab Inc., a private company specializing in antivirus and network security software. Kim Yŏn-su suggests that, aside from correcting deficiencies in the current law, the Republic of Korea does not need any new laws on cybercrime. Prevention is more effective. The author proposes two sets of "Ten Commandments" for protecting personal information on the Internet: one set for users and the other for service providers. The commandments for users mainly provide advice on protecting personal information. For example, users should make sure that they remain informed about how Internet sites use their private information; they should insist that any disclosure of information to third parties occurs only with their consent; and they should install antivirus software. Furthermore, before collecting any personal information from a child who is 14 years old or less, users must obtain permission from the child's legal guardian. The commandments for the providers are, for the most part, a list of obligations. Internet providers should post their privacy policy; they should inform the user and obtain the user's consent for use of personal information

[1] For consistency, the Federal Research Division used the Library of Congress transliteration scheme for Korean, including diacritics and apostrophes. When an author's name appeared in different sources with different transliterations, the researcher noted variants. The conventional order for Korean personal names is family name first.

or transfer of such information to third parties; and they should maintain a firewall and adopt technical and administrative security measures to protect users from viruses.

Paek, Kwang-hun. *Saibŏ pŏmjoe e taehan ISP ŭi hyŏngsa ch'aegim e kwanhan yŏn'gu* [A study on the liability of ISPs]. Seoul: Han'guk Hyŏngsa Chŏngch'aek Yŏn'guwŏn [Korean Institute of Criminology], 2003.

Paek Kwang-hun (variant, Paik Kwang-hoon) is a senior researcher at the Korean Institute of Criminology (KIC). The KIC was established in 1989 under the Korean Ministry of Justice and, in 1999, became a member of the Korean Research Council for Humanities and Social Sciences, as part of the Office of the Prime Minister. In this book, Paek Kwang-hun discusses the criminal liability of Internet service providers (ISPs) for cybercrimes that their users commit. The author argues that, although the government has a duty to protect society from crime, legislation cannot solve the social problems that the Internet has created. Because freedom of expression is a fundamental right that is essential to democracy, ISPs should remain free from excessive government regulation. However, the law should hold ISPs criminally liable for any illegal content that they provide directly, just as criminal law holds any corporation liable for providing illegal articles. When an ISP simply acts as an intermediary, it is not liable for unwittingly transmitting illegal content provided by third parties. However, if an ISP hosts its own network and has the authority to edit, revise, or delete network content, and if that ISP knows that its network is hosting illegal content provided by a third party—content for which the ISP could reasonably be held civilly liable—then the ISP should be held criminally liable. In such a case, the ISP has not done everything that it could reasonably have done to prevent the distribution of the illegal content.

Republic of Korea. National Cyber Security Center (NCSC). *Saibŏ ch'imhae sago sarye punsŏk* [Case studies and analysis of incidents of cyber attacks for 2003]. Seoul, March 2004. Also available online at http://www.kbmge.go.kr/webgear/ board_pds/14/ 20040421153243_2003_cyber_security.pdf (accessed October 8, 2009).

This book, part of a series produced by the Republic of Korea's National Cyber Security Center (NCSC), reports statistics of cyber attacks in the Republic of Korea during 2003. By the end of 2003, the Republic of Korea had 11 million Internet subscribers, and the country's rate of Internet penetration was twelfth in the world. This rapid expansion of the Internet left South Korea vulnerable to cyber attack. On January 25, 2003, a date known as 1/25, the Slammer worm shut down practically all government and private computers in South Korea. This cyber attack hit South Korea harder than any other country. The event also demonstrated South Korea's vulnerability to terrorist cyber attacks. In 2003 South Korea experienced 27,500 cyber attack incidents, an increase of 60 percent over the previous year. The NCSC suggests that, to fulfill its mission to provide adequate cyber security and to prevent another 1/25, it needs sufficient government funding. Moreover, the NCSC needs the private sector to cooperate in promptly reporting incidents of cyber attacks.

Sŏng, Sŏn-je, Yu Chong-hyŏn, and Kang Chang-muk. *Net'ijŭn ŭl wihan e-hŏnpŏp: Cyber law* [An e-constitution for netizens: Cyber law]. Revised edition. Seoul: K'ŏmyunik'eisyŏn Buksŭ [Communication Books], 2006.

Sŏng Sŏn-je is a professor in the Yongsan University law school, Yu Chong-hyŏn is head of the news department at Munhwa Broadcasting Corporation (MBC), and Kang Chang-muk is a professor of computer engineering at the School of Electronic Engineering of Sejong University. Their book discusses threats to private users of the Internet, touching on subjects intrinsic to the nature of cyberspace: pornography, defamation of character, privacy, copyright, and jurisdiction of the courts. The authors describe these problems but do not offer proposals for changes in the law. They argue that the technology of cyberspace has outpaced both the law and the logic of the market. Although the authors discuss pornography in general, they do not mention child pornography. They discuss legislative problems, such as finding the balance between encouraging freedom of expression and preventing harm to society from pornography. Another legal issue addressed is how to determine whether an act constitutes defamation of character, which depends, in large part, on the intent of the perpetrator. The authors discuss privacy in terms of protecting private Internet users from other private users, but they do not discuss the balance between privacy rights and the government's need to protect society. They argue that protection of privacy depends more on technology than the law. Moreover, although they discuss the need to protect copyright and intellectual property, they do not offer legal solutions. Regarding the jurisdiction of the courts, the authors argue that, since cybercrime does not recognize national boundaries, protection against cybercrime requires international cooperation.

Yi, Chŏng-hun. *K'ŏmp'yut'ŏ tŭng sayong sagichoe: Iron kwa chŏgyong* [The crime of fraud using the computer: Theory and application]. Paju: Han'guk Haksul Chŏngbo [Korean Studies Information Company], 2006.

In this book, the author, Yi Chŏng-hun, an assistant professor of law at Chung-Ang University, discusses the Republic of Korea's penal code as it applies to computer fraud. On December 29, 2001, effective June 1, 2002, Article 347-2 was added to Korea's penal code, Law 6543 of 1995. Article 347-2 explicitly made it a crime to use a computer to commit fraud. Yi Chŏng-hun devotes a chapter to comparing Korea's penal code on computer fraud with the penal codes of Germany and Japan. However, although he suggests that those codes are worth studying, he does not recommend that Korea adopt any of their specific provisions in future revisions of its own code. The author suggests that further legislation may resolve disputes regarding the intent of the original legislation and the interpretation of the text of the legislation. Yi Chŏng-hun does not propose any specific new legislation, but he does suggest the necessity of additional legislation to clarify the elements comprising each type of computer crime. For example, the law should indicate what elements constitute the cybercrimes of unauthorized entry, unauthorized editing of data, entry of false information, or malicious commands.

Yu, Yong-bong. *Int'ŏnet pŏmjoe wa hyŏngpŏp* [Internet crime and criminal law]. Paju: 21 Segisa [21st Century], 2005.

Yu Yong-bong, awarded the degree of Juris Doctor from the University of Kiel, Germany, is currently a professor in the Department of Police Administration at Hansei University. His book

discusses, in general, crimes against private users of the Internet in the Republic of Korea and in Germany. Specifically, the author explains the crimes of hacking, infecting computers with viruses, spamming, capturing screen images for illegal purposes, using unauthorized computer programs, cyber stalking, providing or viewing Internet pornography, and online gaming for illegal purposes. The author describes threats to Internet users and cites pertinent legislation in South Korea and Germany. Although Yu does not propose any specific new legislation, he argues that research institutions should devote more study to combating Internet crime. He suggests that government policy should support private enterprise in creating a trained workforce of information personnel; basic military training should include computer training; and primary and secondary school curricula should include moral education.

RUSSIAN AND UKRAINIAN LITERATURE

Akhtyrskaya, N. N. "Organizovannaya prestupnost' v sfere informatsionnykh tekhnologii" [Organized crime in information technology]. [In Russian.] Report, Center for Research on Problems of Computer Crime, Zaporozhye, Ukraine, 2002.

Akhtyrskaya discusses in detail the techniques of investigating cybercrime committed by organized syndicates. The author begins by classifying various types of criminal activity, including individual hooliganism, describing in detail the structure, priorities, and modes of operation of long-term, professional criminal syndicates with complex structures. The author continues with a detailed discussion about the investigation of one of the many types of crime that criminal syndicates commit: cybercrime. Akhtyrskaya lists the characteristics of a cybercrime investigation, such as organizing the investigation and identifying best tactics. She explains the types of information that such an investigation seeks to obtain—for example, information related to the crime itself or information providing clues to the identity of the perpetrator—and the elements of a cybercrime, including the actual act, the type of information compromised, and the results of the act. Akhtyrskaya also discusses the three stages in which law enforcement officers may detect a crime—the incipient, in-progress, and completed stages—and the tasks of the investigator at each stage, such as assembling and evaluating information.

In conclusion, the author warns that cybercrime committed by criminal syndicates tends to be sophisticated, with multiple levels of criminal activity. Therefore, although the investigation of cybercrime lends itself to stepwise analysis and to the listing of components (the components described in the article), the process of investigating it is, typically, fragmentary, complex, and fraught with false leads. Therefore, law enforcement agencies should rely on flexible, heuristic, and creative strategies, rather than on the predetermined strategies that are effective in investigating other types of crime.

Golubev, Vladimir, and Timofey Saymarly. "Problemy bor'by s kiberterrorizmom v sovremennykh usloviyakh" [Problems of fighting cyberterrorism under contemporary conditions]. [In Russian.] Report, Center for Research on Problems of Computer Crime, Zaporozhye, Ukraine, 2002.

With specific reference to Al Qaeda and the events of September 11, Vladimir Golubev and Timofey Saymarly describe the recent development of cyber war as a key weapon of

international terrorist groups, pointing out that terrorists base their use of cyber weapons upon the same philosophy they rely on to justify their use of traditional weapons. Golubev and Saymarly define *cyberterrorism* or *computer terrorism* as a "planned, motivated attack on information processed by computer, or on a computer system or network, constituting a danger to the life or welfare of people or other grave consequences, if such actions are carried out with the goal of destroying societal security, terrifying the populace, or the provocation of military conflict." The authors explain the logic for the use of such tactics, listing types of cyberterrorist attacks, such as computer viruses, techniques of invading computer's control systems and accessing data, and the characteristics of cybercrime that terrorists use to their advantage, such as the ease of concealment. The authors note the effect of the Internet worm VBS/Nedal, which distributed propaganda via the "electronic soil" of Western computer systems. The authors describe two types of cyber attack—direct and remote—characterizing the latter as the more formidable and dangerous.

Because terrorists may use information systems as an ideal weapon for to achieve their aims, information security is a vital aspect of national and international security. Governments should not underestimate the electronic sophistication of terrorist groups: Islamic hackers are a serious threat. Remote attacks—those targeting specific systems or servers from afar—are more dangerous than direct attacks, because remote attacks may have catastrophic global consequences. Thus, cyberterrorism, like organized crime and conventional terrorism, requires governments to respond immediately, using complex approaches. Western countries currently have inadequate personnel trained to combat this type of attack, a lack that they must remedy. Furthermore, Western governments urgently need to streamline their multilayered communications and decision-making apparatus to better address cyberterrorism.

Gutsalyuk, M. V. "Borot'ba z komp'yuternoyu zlochinnistyu yak neobkhidna umova rozvitku elektronnogo biznesu v Ukraini" [The struggle against computer crime as a necessary condition for the development of electronic commerce in Ukraine]. [In Ukrainian.] Report, Center for Research on Problems of Computer Crime, Zaporozhye, Ukraine, 2001.

Gutsalyuk summarizes the rapid growth of computer applications, in a wide range of international business and academic activities, and the parallel growth of various forms of cybercrime. He briefly notes solutions that other countries, such as the Russian Federation and the United States, have formulated. Noting that Ukraine has joined the global trend toward reliance on electronic systems, he states that, so far, Ukraine's system of defense against cybercrime is highly inadequate. He names several of its problems: widely varying definitions of terms and understandings of processes; the lack of hierarchical, clear, and uniform laws—a situation leading to variant legal interpretations; and the enactment of new regulations and laws that are contradictory to existing ones. The author also reports a recent positive development: Ukraine's Interjurisdictional Scientific-Research Center on Problems of Combating Organized Crime has created the Conception for Reform of Legislation on Information Systems. Ukraine's current system of cyber security has many flaws, which are increasing. Gutsalyuk states, "There needs to be coordination between the making of laws on information systems with the real-world requirements of the field, to realize the advantages of electronic communications while ensuring information security both in Ukraine and elsewhere."

Katayev, S. L. "Sotsial'nyye aspekty komp'yuternoy prestupnosti" [Social aspects of computer crime]. [In Russian.] Report, Center for Research on Problems of Computer Crime, Zaporozhye, Ukraine, 2001.

The article comments on Ukraine's new Conception for Reform of Legislation on Information Systems (2000), examining extensively the place of cybercrime in the overall criminal structure of the country, particularly Ukraine's "shadow economy." Katayev proposes that two types of cybercrime are prevalent in Ukraine: 1) the use of computers as a tool for helping criminals smuggle people and illegal goods, or for other conventional criminal activities, and 2) the use of computers to assist individuals in tax evasion. The author suggests that the latter is an inevitable phenomenon in a society in which the instruments and principles of tax collection do not match the social and economic requirements of those expected to pay. The author discusses types of tax evasion, the motivations for each type, and the selective prosecution of tax evaders.

The article also analyzes societal reasons for computer crime, focusing on disparities between the post-modern, organic responsibility associated with the computer world and the traditional understanding of ethical responsibility. Moreover, the disparity between Ukraine's understanding of organic and ethical responsibilities and the understanding of Western Europe and the United States regarding these concepts has led to the misuse of computer technologies—notably, to Ukrainian misuse of Microsoft's technologies. The author proposes that, in Ukraine, the criminal aspects of cyberspace include societal components. The causes of computer crime in Ukraine are societal anomie—the weakness of standards; the transitional nature of Ukrainian society; and the discrepancy that exists in Ukraine between scientific development and the development of ethical responses appropriate to the new technologies.

Computer crime is a part of the overall criminal situation in Ukraine. Ukrainian law-enforcement agencies use specific, electronic methods of combating computer crime, as well as traditional measures of combating crime, such as tax agencies, police, and other punitive and monitoring agencies. Computer crime is a singular kind of payment for progress in the realm of technology. As new computer technologies develop, cybercriminals will also continue to refine criminal activities that use the new technologies. Accordingly, Ukraine must develop systematic methods of combating computer crime—methods that address the societal and ethical aspects of this type of crime.

Nasakin, Rodion. "Kto ikak vymanivayet lichnuyu informatsiyu" [Who obtains personal information illegally, and how they do it]. [In Russian.] *Компьютерра* [Computerra], [after 2004]. http://www.computerra.ru.

Rodion Nasakin describes the rapid growth, since 2000, of the illegal computer activity known as phishing—the technique of illegally obtaining personal electronic identification information, such as passwords, to gain entry into bank accounts and to use credit cards. As of 2004, phishing had become a worldwide form of cybercrime, which had claimed thousands of victims. According to one estimate, one in 20 recipients of an initial phishing message suffered some form of swindle. As phishing crimes became more diverse and sophisticated, preventive

measures lagged behind, and the expansion of this type of cybercrime slowed, but did not end. The first victims of phishing in Russia, swindled in 2004, were Citibank customers.

The author outlines the development of phishing, as the practice became significantly more diverse and sophisticated—the period from the early 1990s until 2004. He describes various methods that phishers use to convince customers to reveal their passwords and personal identification numbers and explains the use of Trojan horses (software that seems benign but in fact provides unauthorized remote access to a computer system) and spyware (software and other devices that gain entrance to a computer system and gather data covertly). Nasakin also describes the role and responsibility of financial institutions in cases of unauthorized use of personal identification. The author documents the recent growth of phishing in the United States, as well as U.S. legislators' efforts to pass laws controlling it, citing Western computer authorities, such as APWG and Symantec, as useful sources for statistics and trends. Finally, Nasakin notes the London trial, in October 2004, of a group of exposed swindlers from the former Soviet Union—the first trial for the crime of phishing. The perpetrators faced the conventional charge of conspiracy to defraud financial organizations and launder money.

Ponomareva, Elizaveta. "Prestupnost' osvaivayet novyye tekhnologii kuda bystreye, chem. pravookhranitel'nyye organy" [Criminals are applying new technology much faster than law enforcement agencies]. [In Russian.] Report, Center for Research on Problems of Computer Crime, Zaporozhye, Ukraine, July 24, 2006.

During the various stages in the evolution of the Internet, individuals have pushed the envelope—eventually stepping beyond the bounds of conventional legal activity. Counter-movements and laws have responded by attempting to control such applications. Article 282 of the Russian legal code, which is apparently a relatively new provision, takes an extreme and unnecessarily strict, albeit incomplete, approach to controlling what has been and likely will continue to be a highly changeable medium. Elizaveta Ponomareva suggests that, no matter what legal measures the government enacts, individuals will continue to find ways around such controls.

Ponomareva traces the development of the popular understanding about what constitutes illegal computer use, relating the changes in this understanding to a variety of potential activities. She considers the process from the standpoint of the organic growth of social forces, rather than that of law enforcement. The author describes the first stages of the development of the Internet, which brought a sense of unlimited freedom. The first stage gave way to a period of vigilante-like self-policing among law-abiding users—in cases of slanderous messaging, for example. Next, outside forces, such as book distributors, began policing the Internet for particular purposes, such as the elimination of electronic access to printed materials. Internet pirates took advantage of the uncertain legal atmosphere to sell unauthorized musical and literary material online. The article concludes with a description of the role of the Russian government and of Russian laws in policing the Internet and the possibility that the government could overstep its authority in this matter.

Shchetilov, A. "Nekotoryye problemy bor'by s kiberprestupnost'yu i kiberterrorizmom" [Some problems in the battle with cybercrime and cyberterrorism]. [In Russian.] Report, Center for Research on Problems of Computer Crime, Zaporozhye, Ukraine, 2001.

In this general discussion of the topic, Shchetilov characterizes cyberterrorism and locates it in the context of overall exponential growth of global cyber communication. Shchetilov's definition of cybercrime includes all types of crime that involve perpetrators' infringement anywhere in the telecommunications sphere. He lists the common types of cybercrime, the strategies that cyberterrorists use, the actual systemic results of illegal intrusion into a computer network, and the distinctive characteristics of cybercrime. Then, he discusses techniques of combating three specific types of cybercrime: illegal access to information stored in global computer networks; crimes using information in other than computer-based electronic forms; and crimes involving distribution of harmful computer programs. For each category, the author discusses the characteristics of the crime and the juridical basis of a finding of guilt. Shchetilov concludes that the goals and methodology of cyberterrorists are the same as those of conventional terrorists: both conduct information wars, propagating their own views as broadly as possible. He also points out that the cyber world is ideal for terrorists because the source of attack is much more difficult to identify than in traditional forms of terrorism. Moreover, combating cybercrime is more difficult than combating traditional types of terrorism, because governments lack technical resources and staff trained to counter cyberterrorism.

Vekhov, Vitaliy. "Aktual'nyye voprosy rassledovaniya prestupleniy, sovershennykh s ispol'zovaniyem plastikovykh kart" [Current issues in investigation of crimes committed using plastic cards]. [In Russian.] Report, Computer Crime Research Center, November 25, 2004. http://www.crime-research.ru.

Vitaliy Vekhov discusses the variety of crimes committed using plastic cards, a type of crime increasing rapidly in Russia, pointing out that investigation of these crimes is not keeping up with this growth. Russia has an insufficient number of people qualified to investigate, assemble evidence, and prosecute crimes involving plastic cards, together with a high volume of card-related cases requiring presentation in court. Police and prosecutors often encounter difficulties in investigations and in the preliminary stages of mounting criminal cases involving cards, because they have an insufficient understanding of the legal status of these cases, of potential criminal misapplication of plastic cards, and of how misuse of cards figures in legal cases.

The author lists the categories of this fast-growing type of crime and explains how the information on plastic cards enables criminals to break into various information systems. Vekhov provides statistics on the financial losses incurred through card-related crimes from 1997 to 2003, noting that Russian law enforcement continues to fall ever farther behind in its efforts to solve such crimes. He analyzes the methodology of investigating crimes using cards, providing a typology for criminological information and for the elements that comprise the investigation. Vekhov also cites a directive of the Central Bank of Russia to identify various types of plastic cards and to explain how they work, providing examples of legal and illegal uses.

Vekhov, Vitaliy. "Opyt bor'by rossiyskikh organov predvaritel'nogo rassledovaniya s DDoS-atakami na servery zarubezhnykh kompaniy" [An example of the struggle of Russian investigative agencies with DDoS attacks on the servers of overseas companies]. [In Russian.] Report, Center for Research on Problems of Computer Crime, Zaporozhye, Ukraine, October 13, 2007.

Vekhov notes the rapid growth in the past 10 years of a distinctive type of cybercrime—distributed denial of service (DDoS). In this type of crime, the perpetrator paralyzes the Web site or computer system of a company that requires timely Internet access to carry on business. Because the victimized company faces enormous financial losses through lost Internet access, the perpetrator is able to demand from the company large sums of money to remove the blockage. Vekhov provides a brief history of the development of DDoS, beginning in 1999. He reports in detail one example of a DDoS operation, which the Embassy of Great Britain reported to the Russian minister of the interior—as a crime that Russian hackers had perpetrated against British transnational bookmaking companies. The article explains the roles of the three main conspirators in the general operation, including measures taken to conceal their identities. In addition, Vekhov provides a detailed account of one specific attack in 2003, an attack targeting companies that ran an Internet scheme that involved betting on the Breeders Cup races.

Zhirniy, G. Yu. "Pro formuvaniya okremikh kriminalistichnikh metodik rozsliduvaniya zlochiniv v sferi vikoristaniya avtomatizovanikh elektronno-obchislyuval'nikh sistem" [On the formation of special investigative methods in the area of computer use]. [In Ukrainian.] Report, Center for Research on Problems of Computer Crime, Zaporozhye, Ukraine, 2000.

Zhirniy discusses approaches to the criminological investigation of computer crimes and how the type of crime dictates those approaches. He insists that law enforcement agencies must carry out their investigations in specific ways, according to these criteria, arguing that attempting to develop an all-purpose methodology, applicable for all types of cybercrime, is useless. Zhirniy bases his classification of criminological approaches on the existing list of cybercrime types provided in the Ukrainian government's Conception for Reform of Legislation on Information Systems (2000). However, he critiques the classification in the 2000 Conception and suggests revisions. For example, he suggests revising the section of the document that describes methods for investigating each step of a crime's commission.

The author proposes five elements of cyber-criminological investigation: the criminal characteristics of the act; the circumstances, as they are understood at the time of investigation; the type of program in use at the time the law was broken; the typology of initial investigative strategy (divided into initial and subsequent steps); and the characteristics of the tactical steps of the investigation itself. He explicates these five elements, citing differences in types of crimes according to their methodology, victim, setting, and motivation. He states that the initial stage of investigation originates from three possible circumstances: the operator of an information system himself reports an illegal act and identifies the perpetrator; the operator reports the act but does not know the identity of the perpetrator; or a routine system check identifies the intrusion into the information system. The author declares that, in view of the methodology he recommends, Ukraine needs an entirely new Conception for Reform of Legislation on Information Systems.

Zhurba, A. I. "Osobennosti obstoyatel'stv sobytiya obshchestvenno opasnogo deyaniya, podlezhashchiye dokazaniyu po komp'yuternym prestupleniyam" [Characteristics of circumstances of a dangerous act subject to proof, as related to computer crimes]. [In Russian.] Report, Center for Research on Problems of Computer Crime, Zaporozhye, Ukraine, December 22, 2005.

In this report, Zhurba examines in detail aspects of a computer crime, explaining the activities of police authorities as they examine and investigate such a crime. The author discusses the elements of a criminal act as stipulated in the Legal Code of Ukraine, as well as examining these elements in the real-life investigation of computer crimes. The elements of a criminal act include the place where the computer crime caused damage; the place from which the crime was committed, in cases of remote computer crime (in cases of direct computer crime, the place of the crime and the place of the damage caused by the crime are identical); the time the crime occurred; and the method and completeness of the criminal act. Zhurba explains the concepts of "circumstances" and "commission" in particular detail. The author compares investigative aspects of the remote and the direct computer crime, referencing several other authorities on his subject and briefly indicating their approaches and contributions.

In a computer crime, unlike other crimes that the Legal Code of Ukraine covers, the perpetrator often commits the crime at a different place from the location where the victim sustains harm or where the damage occurs. Remote crimes constitute the majority of computer crimes. The author considers DDoS crime in an early stage of development and predicts that this type of cybercrime will become more prevalent in the future. Depending on whether the police or civil investigators are seeking the facts, as well as on whether the crime is direct or remote, the investigation of a computer crime may fall into a variety of categories. If some event interrupts a computer crime before its completion, the criminal investigation seeks to establish evidence for the endangerment of public order, rather than for a felony. Russian investigative authorities have had fruitful cooperation with their counterparts overseas, exchanging information and developing strategies to counter DDoS operations.

SWEDISH LITERATURE

Andersson, Helena. "Rättsliga aspekter på myndigheternas informationssäkerhet" [Legal aspects of information security pertaining to public administration]. IRI Promemoria no. 1/2007, Institutet för rättsinformatik (IRI) [Swedish Law and Informatics Research Institute], Juridiska institutionen, Stockholms universitet, 2007. http://www.juridicum.su.se/iri/pdf/IRI-PM%202007-01.sv.pdf.

Helena Andersson explores the extent to which the law may intervene to address information security deficiencies in public administration. She recommends a holistic view, focusing not on the particular sector and its area of responsibility but on the information system that needs protecting, on the likely threats to information security, and on the available protective measures. To address gaps in information security, Andersson suggests changing the law, altering practices, or offering more guidance to the public.

Barck-Holst, Svante, Georg Fischer, and Birgitta Lewerentz. "Underlag för utvärdering av uppgiftsfördelning inom informationssäkerhetsområdet" [Foundations for evaluating information distribution within the information security area]. Report no. FOI-R--1369–SE, Totalförsvarets forskningsinstitut (FOI) [Swedish Defence Research Agency], Stockholm, 2004. http://www.foi.se/FOI/templates/TripAbstract____245.aspx?url=http%3a%2f%2fwww2.foi.se%2fcgi-bin%2fthw%3f%24{BASE}%3drapp%26%24{THWIDS}%3d0.9%2f20449%26%24{html}%3dNewWebAbsEng%26%24{THWURLSAVE}%3d9%2f20449.

In 2001 two existing government agencies, the National Defence Research Establishment (Försvarets Forskningsanstalt—FOA) and the Aeronautical Research Institute (Flygtekniska Försöksanstalten—FFA) merged to form the Swedish Defence Research Agency (Totalförsvarets forskningsinstitut—FOI), a research institute for the study of issues of defense and safety. FOI develops methods for handling dangerous substances and for creating safer information technology systems.

The Swedish government bill, Society's Security and Preparedness (prop. 2001/02:158), allocated new tasks to various government agencies in the area of information security, instructing them to evaluate their area of information security within two years (dir. 2004:46). According to FOI's report, "the Swedish Emergency Management Agency, the National Defence Radio Establishment, the National Post and Telecom Agency, and the Swedish Defence Matériel Administration were appointed responsibilities in [the] respective areas of intelligence collection, technological competence, management of IT-incident reports, and the establishment of a Swedish Scheme for Evaluation and Certification." The report presents base data (problems, issues, and reflections) that the government had instructed agencies to use in their evaluations.

Brottsförebyggande rådet (BRÅ) [Swedish National Council for Crime Prevention]. "Brottsutvecklingen I Sverige fram till år 2007" [Crime developments in Sweden to 2007]. BRÅ-Rapport no. 23, Stockholm, 2008. http://www.bra.se/extra/measurepoint/?module_ instance=4&name=Brottsutvecklingen_webb.pdf&url=/dynamaster/file_archive/081121/8f40c6556f4fb0fbcb0a2d4af6994353/Brottsutvecklingen%5fwebb.pdf.

In this report, BRÅ does not discuss crimes involving information technology separately from other types of crime. On page 164, the report briefly mentions the increase in sex crimes, a phenomenon coincident with the increase in Internet use.

Brottsförebyggande rådet (BRÅ) [Swedish National Council for Crime Prevention]. "IT-relaterad brottslighet" [IT-related crime]. BRÅ-Rapport no. 2, Stockholm, 2000. http://www.bra.se/extra/measurepoint/?module_instance=4&name=00020922854.pdf&url=/dynamaster/file_archive/050121/03b713ce142ff0114eb6e4043f209c5b/00020922854.pdf.

The Swedish National Council for Crime Prevention (Brottsförebyggande rådet—BRÅ) reports that, along with increased Internet use, information technology–related crime in Sweden increased by 50 percent between 1995 and 1999. One in every four organizations has been victimized. Perpetrators primarily targeted the private sector, rather than the public sector.

Information technology–related crime identified in the report includes computer misuse, viruses and other malicious program code, fraud, extortion, gambling, threats and racial slurs, prostitution and child pornography, identity crime, youth crime, copyright violation, smuggling, narcotics and weapons, economic crime, money laundering, organized crime, and information warfare, such as destruction of communications satellites or other threats to security policy. According to the report, the most common cybercrimes are "computer viruses, external and internal computer intrusion, manipulation of data, information theft, and fraud." Although BRÅ views crimes involving information technology simply as another form of law breaking, the Council takes this variety of crime seriously, calling for additional resources to meet the new challenge.

Brottsförebyggande rådet (BRÅ) [Swedish National Council for Crime Prevention]. "Statistik om brottslighet." [Statistics on Crime]. http://www.bra.se/extra/pod/?module_instance=4. Actual table: http://www.bra.se/extra/measurepoint/?module_instance=5&name=/statistik/100/2008/100La-2008.xls&url=/statistik/100/2008/100La-2008.xls.

BRÅ's Web site also features statistics regarding types of online crime, referring specifically to computer-related crime (*dataintrång*) and fraud using computers or the Internet (*datorbedrägeri; med hjälp av Internet*), as well as online child pornography (*Internet-relaterad barnpornografibrott*).

Brottsförebyggande rådet (BRÅ) [Swedish National Council for Crime Prevention]. "Vuxnas sexuella kontakter med barn via Internet" [The online sexual solicitation of children by adults in Sweden]. BRÅ-Rapport no. 11, Stockholm, 2007. English language summary: http://www.bra.se/extra/measurepoint/?module_instance=4&name=04Theonlinesexualsolicitation.pdf&url=/dynamaster/file_archive/070725/aa07fd00144499c249821ad9cc942828/04Theonlinesexualsolicitation.pdf.

In this report, BRÅ presents findings of a study demonstrating an increase in the incidence of online sexual solicitation of children and suggesting preventive measures.

Fylkner, Malin, Henrik Carlsen, Birgitta Lewerentz, Anders E. Eriksson. "Aktörer, antagonister och angrepp—En studie om det kvalificerade IT-hotet" [Actors, antagonists and attacks—A study of specific IT attacks]. Report no. FOI-R--1182—SE, Totalförsvarets forskningsinstitut (FOI) [Swedish Defence Research Agency], Stockholm, 2004. http://www.foi.se/FOI/templates/TripAbstract____245.aspx?url=http%3a%2f%2fwww2.foi.se%2fcgi-bin%2fthw%3f%24{BASE}%3drapp%26%24{THWIDS}%3d0.9%2f9037%26%24{html}%3dNewWebAbsEng%26%24{THWURLSAVE}%3d9%2f9037.

In this study, researchers at FOI define and describe information-technology threats that are of a graver nature than routine IT noise (online chatter), concentrating mainly on threats to national security, but also discussing threats to national interests. The study presents a theoretical framework, categorizing according to their various abilities serious antagonists who act in an information-technology environment. Three scenarios depict how serious information

technology–related threats form the hub of tactical operations. The authors speculate about potential future information technology–related attack scenarios.

Government of Sweden. "Informationssäkerhet I Sverige och internationellt—en översikt" [Information security in Sweden—An overview]. Statens Offentliga Utredningar [Swedish Government Official Report] no. SOU 2004:32, Försvarsdepartementet—Infosäkutredningen [Ministry of Defence—Information Security Analysis], Stockholm, 2004. http://www.regeringen.se/content/1/c6/02/33/50/24f80e10.pdf.

This official report of the Government of Sweden discusses the vulnerabilities of and threats to information security in Sweden and throughout the world. The many parties involved in information protection, including service providers and users, must increase their efforts to cooperate with one another to protect their data systems from threat. Such cooperative efforts are crucial because investigators of information technology–related attacks may find it difficult to trace the source of any specific incursion on a computer system. In addition, service providers and users may have difficulty distinguishing intentional infringements from those that are accidental. Company insiders and subcontractors, industrial spies, foreign states, terrorists, organized crime syndicates, and hackers have varying motives for threatening information security, ranging from promotion of a political agenda to self-interest. Attacks may take the form of physical threats, weapons, viruses, worms, and the invidious and widespread virus attacks that constitute epidemics.

IT-kommissionen [IT-Commission]. "Behandling av personuppgifter och rättsinformationen" [Legal aspects of handling personal data]. Workshop, Stockholm, April 12, 2002. http://www.itkommissionen.se/dynamaster/file_archive/030110/852c2d710e774a42d295a49342c10a0c/pul-seminarium.pdf.

The Swedish IT-Commission is inactive as of 2003 but maintains an online archive of its reports. The IT-Commission did not address cybercrime specifically, focusing instead on information security. This document provides the proceedings of a workshop on the legal issues of securing personal data.

IT-kommissionen [IT-Commission]. "Den fjärde IT-kommissionens arbete" [Work of the fourth IT-Commission]. Rapport no. 70/2003, Stockholm, 2003. http://www.itkommissionen.se/dynamaster/file_archive/030605/7a1feff2d92cafd9389e1d04cdd5e256/Fj%e4rde%20IT-kommissionens%20arbete.pdf.

The IT-Commission reports its findings and activities related to regional training issues, clearer delineation of responsibilities, improved cooperation among government offices, competence in information-resource handling, setting of information standards, design of services, and development of community services and local government services. Other relevant IT-Commission publications include: IT-kommissionen [IT-Commission]. "Den fjärde IT-kommissionens arbete" [Work of the fourth IT-Commission]. Rapport 48, Stockholm, 2002. http://www.itkommissionen.se/dynamaster/file_archive/020814/6d68b28e54b9e867635f7eea8199a061/Verksamhetsber%e4ttelse%202001-2002.pdf.

IT-kommissionen [IT-Commission]. "Grundskydd i datorer och programvaror" [Basic computer and software security]. Report no. 1:2001, PM Observatoriet för informationssäkerhet, Stockholm, 2001. http://www.itkommissionen.se/dynamaster/file_archive/020124/88b3e314955a2e509a2e415aab00ba73/Grundskydd%20i%20datorer%20och%20programvaror.pdf.

The IT-Commission suggests that users need increased technological protection against unauthorized tapping into communications between other parties, unauthorized altering of Internet content, and improper use of online resources.

IT-kommissionen [IT-Commission]. "Säkerhet på Internet: Datavirus och blockering av tjänster" [Safety on the Internet: Computer viruses and denial of service]. Observatorierapport 23/2000, Observatoriet för informationssäkerhet, Stockholm, 2000. http://www.itkommissionen.se/dynamaster/file_archive/020124/4edc090cf3a63a1b6b701a9baa803122/23_2000%20S%e4kerhet%20p%e5%20Internet%20-%20Datavirus%20och%20blockering%20av%20tj%e4nster.pdf.

The report discusses threats to computer systems resulting from the use of unfiltered Internet connections. Examples of such threats include attacks of computer viruses on unprotected computer systems and the inundation of a computer system with an excessive volume of spam, causing DoS. The commission provides general information about detecting threats and protecting against them.

Justitiedepartementet [Swedish Ministry of Justice]. "Angrepp mot informationssystem" [Attacks against the information system]. Proposition 2006/07:66, March 8, 2007. http://www. regeringen.se/content/1/c6/07/86/73/af043821.pdf.

The proposition discusses the amendment of the Penal Code to include specific definitions of wrongdoing and punishment for crime in the computer environment. This is in keeping with the European Union approach.

Justitiedepartementet [Swedish Ministry of Justice]. "Brott och brottsutredning i IT-miljö: Europarådets konvention om IT-relaterad brottslighet med tilläggsprotokoll" [Crime and crime investigation in the information technology (IT) environment: The European Council convention on IT-related crime with added protocol]. Ds 2005:6. http://www.regeringen.se/content/1/c6/03/99/50/9e435101.pdf.

Sweden signed the European Council Convention on Cybercrime in 2001 and an additional protocol in 2003. This memorandum discusses whether Sweden should ratify the convention and protocol, taking into consideration the following needs: 1) the need to harmonize Swedish laws regarding punishment of unlawful use of computers, unlawful monitoring of computer information or electromagnetic emissions from computers or computer systems, data interference, system interference, the misuse of means to commit such crimes, falsification, forgery, child pornography, and the violation of copyright and related rights; 2) the need to develop national decisions on the legal process relating to the crimes addressed in the convention, to develop laws concerning additional information technology–related crimes, and to

use electronic evidence in criminal cases; 3) the need to develop international cooperation in the fight against information technology crime. The memorandum supports ratification of the convention.

Justitiedepartementet [Swedish Ministry of Justice]. "Personal Data Protection: Information on the Personal Data Act." [In English.] Edition 4. 2006. http://www.sweden.gov.se/sb/d/6158/a/74365.

This expands on SFS 1998:204 through amendment 2006:398. While balancing individual rights with freedom of information concerns is important, violations of personal integrity are not permissible. The law must protect personal data with special diligence in the areas of politics and health. Responsibility for data integrity rests with the individual processing personal data. Contravening the Personal Data Act will result in damages or criminal penalties.

Krisberedskapsmyndigheten [Swedish Emergency Management Agency]. "Basnivå för informationssäkerhet (BITS)" [Basic level for information security (BITS)]. KBM rekommendationer 2006:1, Stockholm and Karlstad, 2006. http://www.krisberedskapsmyndigheten.se/upload/8043/bits_rek_2006_1.pdf.

This document recommends administrative security measures for managing public sector intra-organizational information.

Krisberedskapsmyndigheten [Swedish Emergency Management Agency]. "Beredskap mot skadlig kod" [Preparedness against malicious code]. KBM:S temaserie 2005:1, Stockholm and Karlstad, 2005. http://www.krisberedskapsmyndigheten.se/upload/6245/skadligkod_2005-1.pdf.

This study examines preparedness against malicious code in 14 large official Swedish agencies and 10 private enterprises, focusing on incidents involving the introduction of malicious code into the computer systems of these organizations. These incidents mainly affected administrative functions on a short-term basis rather than disrupting core activities. However, the impact on productivity was significant.

The findings indicate that the organizations have improved their information security since 2000, introducing new technologies, such as firewalls, virus protection software, and patches. However, the organizations made these changes mainly in response to specific incidents, rather than as part of long-term planning. Management needs to support these technological solutions by training staff, establishing administrative routines, and increasing staff awareness of vulnerabilities in the information technology environment. Moreover, management needs to risk making functional changes to improve information security. Other concerns addressed in the report include the tension between service demands and security concerns (namely, 24-hour availability of information systems) and vendor limitations.

The study demonstrates that the demand for information security is lower in the private than in the public sector, which has a higher volume of critical information to protect. However, the private sector is more proactive in addressing its concerns than the public sector. Moreover, the

private sector's security requirements are, in fact, comparable to those of the public sector. Furthermore, the private sector has a higher perception of threat from disloyal employees than the public sector does.

Krisberedskapsmyndigheten [Swedish Emergency Management Agency]. "Information Security in Sweden: Situational Assessment." [In English.] Report, SEMA, Stockholm and Karlstad, 2008. http://www.krisberedskapsmyndigheten.se/upload/17461/lagesbedomning_infosakerhet_%202008_eng.pdf.

Criminal activity on the Internet has become progressively more sophisticated. This annual assessment identifies two trends in Internet crime—small and targeted Internet attacks and significant attacks using large networks of commercially leased, hijacked computers. Both types of Internet attack are very costly to society in terms of resources and trust. Organized crime syndicates, significant perpetrators of cybercrime, have substantial resources and, reportedly, exist in China, Hong Kong, Eastern Europe, Russia, and the United States.

The Internet crime of phishing has troubled Sweden's banks since 2006. Malicious code, especially Trojan software, has become more capable of targeting banking systems and more difficult to detect. Individuals are able to obtain botnets commercially, permitting hackers to access bank accounts. Phishers have stolen passwords and succeeded in defrauding individuals. Computer and network failures have also affected the systems of the Swedish government, including the judiciary; Teracom, radio, and television broadcasters; and medical care providers. Junkmail (spam) and viruses constantly bombard computer systems and networks. Individuals and organizations have also reported receiving antagonistic threats, graffiti, and attacks resulting in DoS.

The report points out deficiencies in public-sector information security resulting from organizational deficiencies, such as inadequate policies, command systems, system analyses, or continuity plans. Meanwhile, sectors that depend on time-critical information technology activities, such as the medical care and financial sectors, are increasingly dependent on computer systems and networks, and these sectors require additional security measures. The report suggests that Sweden is inadequately prepared to protect itself against major infrastructure attacks.

Krisberedskapsmyndigheten [Swedish Emergency Management Agency]. "Sveriges beredskap mot nätangrepp" [Sweden's preparedness against net attacks]. KBM utbildningsserie 1/2008, Stockholm and Karlstad, November 30, 2007. http://www.krisberedskapsmyndigheten.se/upload/15926/sveriges-beredskap-mot-natangrepp.pdf. English publication of same report: Krisberedskaps myndigheten [Swedish Emergency Management Agency]. "Large scale Internet attacks." SEMA Educational Series 2008:2, Stockholm, 2008. http://www.krisberedskapsmyndigheten.se/upload/17021/Large%20scale%20Internet%20attacks_utb-ser_2008-2.pdf.

The report discusses three levels of threat, from threats involving limited blocking of access or the manipulation of Internet information, to those that disrupt communications, distort official information, or sabotage critical infrastructure, such as the supply of electricity or water. Sweden

is vulnerable to threats of the most severe kind. Both the Swedish National Audit Office and the Swedish Emergency Management Agency have pointed out shortcomings in the way government authorities responsible for crucial infrastructure handle their own information security. For example, those responsible for essential services lack basic procedures; management is not sufficiently aware of the IT-related vulnerabilities of their systems or of the threat of cyber attack. The Swedish administrative tradition of independent agencies makes it more difficult to develop a comprehensive view of a scenario involving a multifaceted attack. The number of persons qualified to deal with a large-scale attack is limited, and the growing number of broadband connections makes it easier to formulate an attack—to develop a botnet of infected computers, for example. The report, which, for the most part, is a response to the 2007 cyber attack against Estonia, concludes that the Swedish information network is probably sufficiently strong to withstand a total attack of the kind that occurred in Estonia.

Küchler, Markus. "Dataintrång: Om personlig integritet och bevisfrågor" [Computer misuse: On identity security and questions of evidence]. IRI Report no. 2000:1, Institutet för rättsinformatik (IRI) [Swedish Law and Informatics Research Institute], 2000. http://www.juresjofart.se/ns/default.asp?url=visatitel.asp?tuid=200.

Markus Küchler discusses illegal computer use and the related contemporary legislation (Penal Code Chapter 4, Para. 9c). Küchler studied questions of evidence in a situation in which legal authorities could not use undercover surveillance but, instead, had to rely on information from the electronic service provider and from house searches.

Riksrevisionen [Swedish National Audit Office]. "Regeringens styrning av informationssäkerhetsarbetet i den statliga förvaltningen" [Government management of information security in national administration]. Report RiR 2007:10, Stockholm, 2007. http://www.egov.nu/uploaded/RiR_2007_10_Reg_och_informationssakerheten.pdf.

The Swedish National Audit Office reports that the Swedish government has not done enough to protect information security or to follow up on the measures that various government authorities have taken in this area. An examination of 11 authorities revealed that, because of a lack of oversight and an incomplete understanding of the various information security requirements and regulations, the government agencies have failed to provide adequate protection for their information technology systems. Serious incidents, which the agencies have failed to address, include virus attacks, defacement of homepages, and lengthy downtime during changes and updates to information technology systems. The audit calls for the government to increase its attention to issues of information security, to provide authorities with a clear mandate to secure information systems, and to formulate clearer requirements for the protection of information systems.

The responsibility for leading and guiding information security in the public sector rests with the Swedish Parliament, government, and individual government authorities. The 11 units included in this study were the Swedish Public Employment Service (Arbetsmarknadsverket—now Arbetsförmedlingen), Social Insurance (Försäkringskassan), Land Survey Administration (Lantmäteriet), Swedish Migration Board (Migrationsverket), National Government Employee Pensions Board (Statens pensionsverk), Swedish Maritime Administration (Sjöfartsverket),

Swedish Companies Registration Office (Bolagsverket), Swedish Armed Forces (Försvarsmakten), Swedish Post and Telecom Agency (Post- och telestyrelsen), Swedish Civil Contingencies (Beredskap), and the State Electric and Gas Utility (Svenska kraftnät).

Stenström, Paula. "Vilseledning på Internet" [Deception on the Internet]. Styrelsen för psykologiskt försvar, Gunnar Sjöstedt [Swedish National Board of Psychological Defence], 2002. http://www.psycdef.se/templates/PublicationItem____279.aspx.

Nobody is able to guarantee that Internet information is correct. This study explores ways that perpetrators could misuse the Internet deliberately to threaten democracy and national security. The author discusses 16 different incidents and the techniques that the perpetrators used to cause harm, drawing attention to existing vulnerabilities that permit the misuse of the Internet. Incidents that have occurred, with harmful consequences, include the following:

- Dissemination of false news (e.g., the headline, "Pol Pot in Sweden");
- Dissemination of false information about a product (e.g., the report of an unsafe airplane)
- *Hacktivism*—Politically motivated hacking into an organization's computer system to cause damage or threatening to do this
- Dissemination of false information about an organization
- Dissemination of false personal information (e.g., slander of a former girlfriend)
- Pretending to be a well-known political figure, thereby obtaining attention or information
- Dissemination of false information about the future value of a company's shares
- Dissemination of false information about public figures in a chain e-mail, resulting in the named individual receiving a large number of unwanted responses
- Sending responses to a business address, based on entirely false information, for political gain
- Dissemination of incorrect information about a business, leading to a drop in the value of the company's shares
- Dissemination of a false chain e-mail about a fictitious apartment lottery, resulting in ill will toward a particular business
- Dissemination of a false chain e-mail about a fictitious Volvo lottery
- Dissemination of a false chain e-mail request for child pornography, resulting in the person whose e-mail address was hijacked receiving hate mail
- Creating a close copy of a known Web site with the addition of misleading information
- Adding misleading information to a preexisting Web site
- Dissemination of propaganda disguised as legitimate news
- Dissemination of a fake press release about a company's situation, resulting in a drop in the value of the company's shares

Westman, Daniel. "Förslag på nya civilrättsliga sanktioner I kampen mot olaglig fildelning—En kritisk granskning" [Suggestions for new civil law sanctions in the fight against unlawful file sharing—A critical study]. IRI Promemoria no. 2007:3, Institutet för rättsinformatik (IRI) [Swedish Law and Informatics Research Institute], 2007. http://www.juridicum.su.se/iri/pdf/IRI-PM_2007-03.pdf.

Daniel Westman critiques two proposed laws regarding illegal file sharing. According to the first proposed law, in a case in which perpetrators have used an electronic-service subscription to infringe intellectual property rights, a court may order the provider of the electronic service not to disclose to the intellectual property owner the name of the account subscriber. Under the second proposed law, electronic-service providers could terminate the service of those whose accounts have been repeatedly used to violate copyright law. (On December 12, 2008, the Swedish Parliament rejected a related proposal, Motion 2008/09:N.)

APPENDIX: ADDITIONAL SOURCES

Additional Chinese Material

Newspaper Article

Qingdao Daily. "Cybercrime: The nightmare of the Internet age." May 29, 2007. http://news.xinhuanet.com/internet/2007-05/29/content_6167344.htm.

In the 21st century information age, people in China have become increasingly accustomed to using the Internet for chatting, shopping, and entertainment. However, criminals have also increased their used of the Internet as a tool for crime, using it to target potential victims. Individual and commercial Internet users encounter the nightmare of computer viruses that cause inestimable damage. Statistics of the Internet police branch of the Qingdao Municipal Police Department indicate that approximately 30 percent of police reports are from individual users and small or medium-sized enterprises who reported that worms and Trojans had infected their computers. In addition to perpetrating hacker attacks, criminals have increased their use of the Web for activities such as pornography, commercial and credit card fraud, and film and music piracy. Currently, diverse types of cybercrime violate the financial and personal rights of individuals. Cybercrime is covert, occurs continuously, and has no national boundaries. Cybercriminals are no longer expert hackers; gradually, perpetrators possessing only basic computer knowledge have succeeded in causing serious damage. Security organizations recommend combating cybercrime by providing more secure Web administration; educating the public about legal issues involved in Internet use; standardizing and modernizing Internet police forces; and invoking the active cooperation of the entire society, especially the telecommunications sector and the police.

Additional Dutch Material

Journals

The following are Dutch-language journals that publish articles on legal, computer science, and other analyses of cybercrime. However, these journals are not peer-reviewed.

Beveiliging [Security]
Computerrecht [Computer law]
I & I: Nieuwe media in perspectief [I and I: New media in perspective]
Informatiebeveiliging [Information security]
ITeR (*Informatietechnologie en recht*) [Information technology and law]
Livre [Book]
Privacy en informatie [Privacy and information]
Strafrecht en ICT [Criminal law and information and communication technology (ICT)]

Conferences

Cybercrime Symposium, December 6, 2007.

What the Hack, July 28 to 31, 2005
Workshop on Secure Multiparty Computations (SMP), Amsterdam, the Netherlands, October 7 to 8, 2004.

Organizations

The following organizations perform research on cybercrime exclusively, or they are composed of individuals who have published academic research on cybercrime. Some individuals have affiliations with more than one of these organizations.

Center for CyberCrime Studies (Cycris)
Center for Mathematics and Computer Science, Amsterdam
Criminal Law Institute, University of Nijmegen
Department of Information and Computing Sciences, Utrecht University
Digital Security Group, University of Nijmegen
Faculty of Computer Science, Free University of Amsterdam
Faculty of Electrical Engineering, Mathematics, and Computer Science, Twente University
Faculty of Mathematics and Computer Science, Eindhoven University of Technology
Faculty of Mathematics and Computer Science, University of Groningen
Information and Knowledge Systems Group, University of Nijmegen
Security of Systems Group, University of Nijmegen
Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University

Web Sites

Centre for Cybercrime Studies
Digital Security Group, University of Nijmegen

Additional Italian Material

Online Articles

Frediani, Valentina. "Antivirus, non aggiornare è reato" [Antivirus, not keeping up-to-date is a crime]. *Punto Informatico* [Computer Point], April 21, 2009. http://punto-informatico.it/2605138/PI/Commenti/antivirus-non-aggiornare-reato.aspx.

This article by Valentina Frediani, dated April 21, 2009, reports that the Italian court found the municipal government of Milan guilty of not using the latest available methods to protect the city's computer records safe from viruses and forced the city to pay a large fine.

Minotti, Daniele. "Sed lex/Se il worm è accesso abusive" [Sed lex/Se the worm is illegal access]. *Punto Informatico* [Computer Point], May 16, 2008. http://punto-nformatico.it/2288187/PI/Commenti/sed-lex-se-worm-accesso-abusivo.aspx.

Minotti's article, dating from May 16, 2008, discusses the recent finding of the appeals court in Bologna that a young Italian man who introduced a computer worm called Vierika into the

Internet in 2001 is guilty of a crime according to Italian law. This was the first time a case of this kind had gone to trial in Italy.

Uricchio, Marcella. "Transazioni online e criminalità informatica" [Online transactions and cybercrime]. Leggi e Norme [Law and Norms], *PMI.it*, June 22, 2007. http://www.pmi.it/leggi-e-norme/articoli/1056/transazioni-online-e-criminalita-informatica.html.

The article deals with the risks connected with online business transactions. Europeans have passed legislation to address transactions of this kind but often in a piecemeal fashion, leaving gaps and presenting interpretive difficulties. Because partners in a transaction are often from different countries, it is sometimes difficult to judge which country's laws apply to the case. So-called sniffer programs (programs that monitor network traffic) allow outsiders to learn sensitive information. The article lists other threats: password cracking, phishing, viruses, and wardriving (using a portable computer to search for wireless networks while driving in a car). In Italy, combating computer crimes is the responsibility of the highly specialized agents of the Polizia Postale e delle Comunicazioni (Postal and Communications Police).

Vizzarro, Danilo. "I reati informatici" [Computer crimes]. *Mibmagazine*, March 13, 2006. http://www.mibmagazine.it/article.php?id=72.

Vizzarro's article is an overview of computer crime and the types of criminal activities that make up computer crime. Most of the article covers Italian legislation regarding cybercrime, including a list of the main laws. The author summarizes the penalties for various kinds of criminal acts and identifies the increased sanctions that may apply in aggravating circumstances. For example, intrusions into military networks may result in sentences carrying a confinement of as much as eight years. Although the Italian government updates regulations regarding cybercrime frequently, technical developments are so rapid that the law has difficulty keeping pace with them. Moreover, computer crime has certain complicating elements: the authors of a cybercrime are frequently difficult to identify; different countries have different laws; cybercriminals are adept at concealing their identities by using the personal data of innocent people; and the number of cases of cybercrime in which courts have handed down sentences remains small.

Conference Presentations

Conferenza internazionale su strumenti, procedure, standard operativi e ricerca accademica nel settore delle investigazioni su Internet con speciale riferimento alla child pornografia [International conference about tools, procedures, standard operations and academic research about investigations on the Internet with special emphasis on child pornography], Rome, May 23, 2005.

The online magazine of the Italian national police force, the Carabinieri, has published talks presented at the International conference about tools, procedures, standard operations and academic research about investigations on the Internet with special emphasis on child pornography (Conferenza internazionale su strumenti, procedure, standard operativi e ricerca accademica nel settore delle investigazioni su Internet con speciale riferimento alla child pornografi). These talks are available online in both Italian and English:

Grammarota, A. "Steganografia e Steganalisi" [Steganography and steganalysis]. English-language version: http://www.carabinieri.it/Internet/Arma/Oggi/Convegni/Roma23052005/23+maggio/04_n.htm.

Mancuso, Luigi. "Operazione 'Falcon—USA-Italia e Operazione 'Twins'—EUROPOL-Italia" [International child pornography investigation. Cases study]. English-language version: http://www.carabinieri.it/Internet/Arma/Oggi/Convegni/Roma23052005/23+maggio/11_n.htm.

Mattiucci, Marco. "Investigazioni Tecniche: Mezzi e problematiche" [Technical investigations: Tools and procedure]. English-language version: http://www.carabinieri.it/Internet/Arma/Oggi/Convegni/Roma23052005/ 23+maggio/08_n.htm.

Strano, Marco. "Protocollo di investigazione sotto copertura per la pedo-pornografia su Internet" [Protocols of undercover investigation of child pornography on the Internet]. English version: http://www.carabinieri.it/Internet/Arma/Oggi/Convegni/Roma23052005/23+maggio/09_n.htm.

Vanina, Roberta. "La coordinazione d'inchieste in materia di pornografia infantile presso lapolizia giudiziaria federale" [Coordinated child pornography investigations]. English-language version: http://www.carabinieri.it/Internet/Arma/Oggi/Convegni/Roma23052005/23+maggio/15_n.htm.

Online Periodicals

Computerlaw informatica e diritto [Computer science and law]. http://www.computerlaw.it/.

The online journal *Computerlaw informatica e diritto* publishes articles, information, and commentary about many aspects of law relating to computers. Topics covered include communications law, e-copyright, e-privacy, e- commerce, and computer crimes.

Crimine.info [Crime.info]. http://www.crimine.info/index.html.

Crimine.info is an online magazine directed by the attorney Leo Stilo and dedicated to examining cybercrime from three standpoints: legal, technical, and criminological. *Crimine.info* furnishes relevant legislation of Italy and of the Council of Europe. Until at least the summer of 2007, the online magazine reported the most recent amendments to Italian law. *Crimine.info* also provides definitions of many types of computer crime, such as card sharing (impersonating a cardholder online to share access to television service cards), cybersquatting (using the domain name of another individual or entity with the intent to profit), denial of service (DoS), and spoofing (masquerading online as another person, program, or Web site). Stilo's Web site also advises on how to report a computer crime to law enforcement authorities in Italy.

Mibmagazine. http://www.mibmagazine.it/index.php.

Mibmagazine is an Italian computer magazine published online. Its editors and writers are all well versed in computer technology.

Punto Informatico [Computer Point]. http://punto-nformatico.it/.

Punto Informatico is an online journal with sections on news relating to the Internet, security, technology, digital life, law and the Internet, and the market. The section on law (*dritto*) and the Internet includes dozens of articles about cybercrime, which the magazine has published over the last few years.

Web Sites

Anti-Phishing Italia. http://www.anti-phishing.it/.

This impressive up-to-date, privately run Web site, which designates itself as the portal against online fraud, publishes articles on Italian cybercrime. Anti-Phishing Italia covers this variety of crime in general, as well as reporting specific incidents throughout Italy. The site also hosts videos that the Italian government has produced to provide public information about online crime and about how people can protect themselves from cybercrime.

Citta di Torino, Polizia Municipale di Torino, Sicurezza Urbana, Reati Informatici [City of Turin, Municipal Police of Turin, Urban Security, Computer Crime]. http://www.comune.torino.it/poliziagiudiziaria/nis/reati_informatici/.

The municipal police of Turin publish this Web site about cybercrime as a public service. Sections of the site publish information about how ordinary computer users can defend themselves against viruses, worms, Trojans, dialers (programs that make unauthorized telephone calls), spam, and spyware. The site offers links to several free tools, which users can download. The Web site also provides copies of Italian legislation regarding computer crime, as well as a long glossary of computer terminology and a set of answers to frequently asked questions (FAQs). Some of the FAQs answered on the site explain how to tell whether an e-mail message contains a virus, whether a perpetrator has installed a dialer in one's computer, and whether one's computer is secure after the installation of antivirus software.

Fondazione Ugo Bordoni [Ugo Bordoni Foundation]. *Ricerca e consultenza nel settore dell'ICT* [Research and consultation in the information and communication technology (ICT) sector]. http://www.fub.it/en/aree/sicurezzaict.

For a number of years, this quasi-statal foundation has concerned itself with many aspects of the information and communication technology (ICT) sector, including information and communications security. The foundation presents its work in this field as follows:

The [Foundation] collects and develops skills about ICT security with special emphasis on technical aspects. The purpose of ICT security is to protect confidentiality, integrity, and

availability of data and services in information systems and TLC systems against damaging events that can be intentional (attacks) or accidental. The protection tools (countermeasures) used to reduce both the probability of damaging events and the extent of the damage they produce are selected by methodologies of risk analysis and risk management. Countermeasures may be organizational (e.g., company policies for managing ICT security and associated procedures, as selection of personnel and allocation of roles and responsibilities), physical (e.g., armored doors and unbreakable containers) and technical (i.e., implemented in hardware, software and firmware). Technical aspects of ICT security, on which the [Foundation] essentially focuses, include selection (within risk analysis and risk management), design, implementation, installation, configuration, and testing of technical countermeasures (security functions).

The Ugo Bordoni Foundation sometimes publishes articles on computer security in its serial *Quaderni di Telema* (http://www.fub.it/en/pubblicazioni/quadernitelema/ LenuovefrontierEdellapirateriaedellacriminalitainformatica).

The issue of July–August 2005 was entitled *Le Nuove frontiere della pirateria e della criminalita informatica* (New frontiers of pirating and computer criminality). Articles in that issue dealt with the problems of peer-to-peer communication, cell-phone viruses, and investigative strategies in the fight against computer crime, as well as providing an overview of the various operating systems' preparedness against breaches of security.

Polizia di Stato Technolgie Polizia Postale [National Police Technologies Postal Police]. http://poliziadistato.it/articolo/747-phishing_un_e_mail_per_rubare_i_vostri_dati_ di_home_banking.

This Web site of the Italian Postal Police furnishes information about how to protect oneself from computer crime. In June 2009, the site provided information about phishing, fraud using eavesdropping technologies, and the cloning of credit cards, as well as information about the Child Exploitation Tracking System (CETS), a tool to catch pedophiles using the Web.

University of Perugia Mathematics and Informatics Department Cyber-Crime Working Group. https://www.cybercrimeworkingroup.org/ Home/HomeEng/tabid/136/Default.aspx.

This is the Web site for the Cyber-Crime Working Group, established in March 2005 by researchers at the University of Perugia Mathematics and Informatics Department. The site provides information about a number of topics related to computer crime, including recent examples of such crimes in Italy, information about the varieties of computer crime, and relevant Italian legislation. The working group also conducts seminars, conferences, and international symposia on cybercrime and cyberterrorism and supports foreign organizations in their work on cybercrime.

Additional Japanese Sources[2]

Abe, Makoto. "Current issues and measures for prevention of cybercrime—Prosecution of cybercrime." *Keisatsu jihō* [Police times] 62, no. 2 (February 2007): 13–24.

[2] These articles are not available in the United States.

Association for Information Service Industries: International Branch. “International trends in measures against cybercrime and the establishment of information security.” *JISA Bulletin* 63 (October 2001): 77–90.

Danjoh, H. “A consideration of evidence-collection activities in the computerized society.” [In English.] *Cyuou hougaku rebyu* [Chuo law review] 113, nos. 3–4 (January 1, 2007): 175–201.

Hamada, Kazuyuki. “Window on the world from the U.S.A.: The spread of damages from cybercrime’s new industrial wave.” *Sangyō shinchō* [The new wave of industry] 55, no. 4 (April 2006): 26–28.

Hashimoto, Naoki. “Current issues and measures for prevention of cybercrime.” *Sōsa kenkyū* [Investigation research] 56, no. 2 (February 2007): 20–29.

Hashimoto, Naoki. “Current issues and measures for prevention of cybercrime.” *Valiant* 25, no. 4 (April 2007): 9–16.

Hayashi, Yōichi. “Indecent content and criminal law.” In “Cybercrime now.” Special issue, *Gendai keiji hō* [Current criminal law] 6, no. 1 (January 2004): 6–10.

Honda, Naohiro. “Current issues and measures for prevention of cybercrime: Current status, etc.” *Keisatsu jihō* [Police times] 60, no. 12 (December 2005): 15–21.

Ibusuki, Makoto, Kouki Tachiyama, and Masao Tatesaki. “Symposium on network security and cybercrime.” *Iyōhō netto wāku, rō re vyū* [Information network law review] 1 (March 2003): 72–95.

Ishii, Tetsuya. “Keynote of the cybercrime convention in Japan.” *Nara hogakkai zasshi* [Nara law review] 15, nos. 1–2 (September 2002): 47–58.

Ishikawa, Ryosuke. “Benefits of a cyber society: Measures and trends of cybercrime in the [United States] and Japanese concerns.” In “Cyberterrorism scenarios.” Special issue, *Chian foramu* [Security forum] 9, no. 1 (2003): 2–12.

Ishikawa, Ryosuke. “Benefits of a cyber society: Measures and trends of cybercrime in the [United States] and Japanese concerns.” In “Cyberterrorism scenarios.” Special issue, *Chian foramu* [Security forum] 9, no. 2 (February 2003): 95–103.

Ishikawa, Ryosuke. “Effects of a cyber society—Current status and measures against cybercrime and cyberterrorism in the [United States] and Japanese concerns.” In “Cyberterrorism scenarios.” Special issue, *Chian foramu* [Security forum] 9, no. 3 (March 2003): 82–90.

Ishikawa, Ryosuke. “Effects of a cyber society—Current status and measures against cybercrime and cyberterrorism in the [United States] and Japanese concerns.” In “Cyberterrorism scenarios.” Special issue, *Chian foramu* [Security forum] 9, no. 4 (April 2003): 64–73.

Ishikawa, Ryosuke. "Effects of a cyber society—Current status and measures against cybercrime and cyberterrorism in the [United States] and Japanese concerns." In "Cyberterrorism scenarios." Special issue, *Chian foramu* [Security forum] 9, no. 5 (May 2003): 47–54.

Ishikawa, Ryosuke. "Effects of a cyber society—Current status and measures against cybercrime and cyberterrorism in the [United States] and Japanese concerns." In "Cyberterrorism scenarios." Special issue, *Chian foramu* [Security forum] 9, no. 6 (June 2003): 35–43.

Iwakuma, Michihiro, and Horibe Masao. "Shin intānetto to ho (3) saibā hanzai saibā sensō no kokusai teki sakumen" [The Internet and the law no. 3: International cybercrime, cyber war]. *Conpyutā tude* [Computer today] 19, no. 1 (January 2002): 52–59.

Japan. Ministry of Economics and Industry. "The European Council's Convention on Cybercrime and measures that our nation should take regarding cybercrime." Report, Association for Cyber Criminal Law, Tokyo, 2002.

Japan. National Police Agency. "Occurrences of illegal access and research on and development of access control mechanisms." Statistics on cybercrime, Heisei 18th [18th Conference] of the National Police Agency, 2007.

Japan. National Police Agency. "On the status of prosecutions of cybercrime and requests for consultation on cybercrime." Heisei 18th [18th Conference] of the National Police Agency, 2006.

Japan. National Police Agency. "On the prosecution of cybercrime." Heisei 19th [19th Conference] of the National Police Agency, 2008.

"Japanese companies lack protection against economic cybercrime—Industry spying on networks and cyberspace: The dangers of stock price manipulation." *Verdad* [Truth] 6, no. 8 (August 2000): 36–37.

Kato, Masayasu. "Current issues on security measures for illegal information and hazardous information on the Internet." In "Cybercrime." Special issue, *Keisatsu koron* [Police public opinion] 62, no. 12 (December 2007): 23–29.

Koch, Christopher. "Security guidance: Preparing for the sophistication and expansion of cybercrime—Computer security issues should now be treated as a 'business risk'." *CIO* 9, no. 3 (March 2008): 70–77.

Kodama, Seiji. "Strengthening measures against cybercrime." *Sōsa kenky*ū [Investigation research] 53, no. 8 (August 2004): 54–58.

Kodama, Seiji. "Strengthening measures against cybercrime." *Valiant* 22, no. 9 (September 2004): 15–19.

Koyato, Wataru. "Prefatory note on current issues and measures for prevention of cybercrime." *Keisatsu koron* [Police public opinion] 59, no. 11 (November 2004): 12–16. In "50 years of law enforcement." Special issue, *Keisatsugaku ron syū* [Papers on police studies] 57, no. 7 (July 2004): 142–55.

Kumono, Yasunari. "Evolving cybercrime and the necessity of the 'PCIDSS' [PCI Security Standard Council]." *Gekkan shyohisha shinyō* [Consumer trust monthly] 26, no. 10 (October 2008): 50–54. To learn more about the PCIDSS, please see https://www.pcisecuritystandards.org/.

Livesley, Andrew. "The establishment of a serious organized crime agency and countermeasures against cybercrime." [In English.] *Keisatsu seisaku kenkyu* [Police policy research] 11 (2007): 84–92.

Masuda, Kōichi. "Pondering cybercrime." *Keisatsu koron* [Police public opinion] 63, no. 7 (July 2008): 4–6.

Nakanome, Yoshinori. "Studies of cybercrime victims." *Higaishagaku kenkyū* [Japanese journal of victimology] 14 (March 2004): 41–50.

National Police Agency, Information Technology Analysis Division, Research Analysis Measures Section [Keisatsu chō Jyohogijyutsu kaisekika gijyutsy taisaku kenkyū kai]. "Basic courses on measures for cyberterrorism investigation." *Sōsa kenkyu* [Investigation research] 53, no. 6 (June 2004): 62–70.

Natsu, Takahito. "Main issues surrounding the Convention on Cybercrime." Research group article, Law Institute at Meiji University Research Group. *Horitsu ronhyo* [Discussion papers on law] 75, 2–3 (December 2002): 261–66.

Ogura, Toshimaru. "Globalization of the Convention on Cybercrime and police power." In "Global militarism." Special issue, *Impakushion* [Theory for change] 125 (2001): 52–66.

Okada, Yoshifumi. "Regulations on hacking and cracking." In "Cybercrime now." Special issue, *Gendai keiji ho* [Recent criminal law] 6, no. 1 (January 2004): 35–39.

Okanishi, Kenji. "Current issues and measures for prevention of cybercrimes: Trends in the regulation of laws regarding computer-related crimes." *Pasokon retarashi* [Personal computer literacy] 30, no. 3 (March 10, 2005): 12–17.

Ono, Masahiro, Donald Andy Purdy, and Akira Saka. "Responses: Panel discussion: summary." Police Policy Forum on Cybercrime—Measures for the prevention of cyberterrorism. *Keisatsu seisaku kenkyu* [Police policy research], 2007, 98–111.

Ono, Yoshihiko. "Award-winning submission considering the establishment of the Asian Society for Information Security—Cybercrime in Asia: On managing the risks of cyberterrorism." *Rikkyo journal of social design studies* 3 (2004): 65–74.

Ōsugi, Mitsuko. "What is a 'safe society'? Pondering recent criminal legislation." [In English.] *Agenda* 5 (June 2004): 102–105.

Ou, Shian. "Legality of computer investigation—Issues not addressed in the Convention on Cybercrime." *Komazawa hogaku* [Komazawa law and political science review] 3, no. 3 (March 2004): 114–32.

"Policy flash: Offering the world an 'active plan to realize a crime-resistant society', to revive Japan, and to make the country safe." Statement of Masahide Maeda, Tokyo Metropolitan University Law School. *Toki no ugoki* [Movement in time] 48, no. 2 (June 2004): 2–9.

Purdy, Donald Andy. "Critical infrastructure protection in the United States." *Keisatsu seisaku kenkyu* [Police policy research] 11 (2007): 77–83.

Satō, Takashi, and Mari Takano. "Promotion of measures against cybercrimes: The establishment and reorganization of the Office for the Prevention of Cyber and IT Crimes." In "The reorganization and future proceedings of the Ministry of the Police." Special issue, *Keisatsu koron* [Police public opinion] 59, no. 9 (September 2004): 38–43.

Schwarzenegger, Christian. "Lecture on the implementation of the Treaty on Cybercrime in Germany, Austria, and Switzerland on November 23, 2001." [In English.] *Jyōhō netto wāku, rō re vyū* [Information network law review] 1 (March 2003): 3–31.

Schwarzenegger, Christian, Natsui Takato, and Kasahara Takehiko. "Central issues on network and law." The Convention on Cybercrime (November 23, 2001) for the International Harmony of Computer Crime Laws and Internet Crime Laws. *Hanrei taimuzu* [Times precedents] 54, no. 4 (February 15, 2003): 70–78.

Shibata, Kensuke, Yosuke Aragane, Shinsaku Numata, Itaru Kamiya, Kazutoshi Sano, and Atsushi Kanai. "An approach for a damage-process model of social engineering regarding cybercrime." *IPSJ SIG Notes* (Information Processing Society of Japan Special Interest Group), May 15, 2008, 79–84.

Sonoda, Hisashi. "Recent cybercrimes." In "The prevention of student subjection to falsified consumer agreements." Special issue, *Daigaku to gakusei* [University and students] 17 (July 2005): 14–21.

Sonoda, Hisashi. "Treaty on Cybercrime." [In English.] *Nomos* [Sociology] 13 (December 25, 2002): 417–24.

Sonoda, Hisashi. "The Convention on Cybercrime." In "International crime, details of crimes by foreign nationals." Special issue, *Gendai keiji ho* [Recent criminal law] 3, no. 9 (September 2001): 29–35.

Shizume, Motoki. “Criminal responsibilities of providers, etc.” In “Cybercrime now.” Special issue, *Gendai keiji hō* [Current criminal law] 6, 1 (January 2004): 17–27.

Tadaki, Makoto. “Cybercrime and crime locations.” In “Cybercrime now.” Special issue, *Gendai keiji hō* [Current criminal law] 6, no. 1 (January 2004): 28–34.

Takahashi, Mamoru. “Lecture 1: Trends in cybercrime and measures against cyberterrorism.” Security Seminar report, Heisei 15th [15th Conference], Market Information Systems Center. *Kinyu sisutemu* [Financial information systems] 270 (2004): 186–204.

Takinami, Hirofumi. “On the Convention on Cybercrime—The Act (Part 2): Agreement on international cooperation and procedure.” *Keisatsugaku ron syū* [Papers on police studies] 55, no. 11 (November 2002): 105–25.

Takinami, Hirofumi. “Trends in criminal legislation: On signing the Convention on Cybercrime.” *Gendai keiji ho* [Current criminal law] 4, no. 6 (June 2002): 70–81.

Tasaka, Shigeki. “Information society and ethics.” *Annual report of Gifu University*, Japan, March 2003, 37–94.

Tomita, Kunitaka. “Investigation on the application of repurchasing cybercrimes.” *Sōsa kenkyū* [Investigation research] 56, no. 3 (March 2007): 11–16.

Tomita, Kunitaka. “Investigation on the application of repurchasing cybercrimes.” *Valiant* 25, no. 5 (May 2007): 9–13.

Watanabe, Akira. “Current issues in the investigation of cybercrimes.” In “Cybercrime.” Special issue, *Keisatsu koron* [Police public opinion] 62, no. 12 (December 2007): 14–22.

World Digest European Council. “Settling the final proposal for the Treaty on Cybercrime.” [In English.] *Overseas Telecommunications Journal* 34, no. 1 (April 2001): 45–50.

Yamagami, Naoyuki. “Measures against cybercrimes in our nation in relation to the European Council’s Convention on Cybercrime.” *Hōgaku jānaru* [Law journal] 19 (March 2004): 179–94.

Yamaguchi, Atsushi. “Current issues regarding cybercrime.” In “Cybercrime now.” Special issue, *Gendai keiji hō* [Current criminal law] 6, no. 1 (January 2004): 4–9.

Yamaguchi, Atsushi. “Proposal for amending the legislation for the Convention on Cybercrime.” *Hō to gijyutsu* [Law and technology] 26 (January 2005): 4–11.

Yao, Akira. “The Council of Europe’s Deliberations regarding the Convention on Cybercrime.” *Osaka shōgyō daigaku ron syū* [Osaka University of Commerce bulletin] 133 (June 2004): 77–99.

Yasutomi, Kiyoshi. "Proceedings: Cybercrimes and information security." *Journal of Kanazawa Seiryo University* 38, no. 3 (March 2005): 49–56.

Yoshida, Kazuhiko. "Official report on current issues and prevention of the damages from cybercrime." [In English and Japanese.] *Gekkan kinyū jā naru* [Monthly financial journal] 47, no. 2 (February 2006): 44–50.

Yoshimura, Katsumi. "Against illegal multimedia invasions—Japan that is not protected against cybercrime." *JMA manejimento rebiu* [JMA management review] 6, no. 7 (July 2000): 42–45.

Additional Swedish Sources

Swedish Public Law

Swedish legislation, such as criminal law and libel law, also apply to issues of information security and the fight against cybercrime, regardless of the context in which the crime takes place. Frequently, the law has focused on information security rather than cybercrime, but with the increase in computer use, the legislature has also passed Internet-specific laws.

SFS 1960:729 Lag (1960:729) "Om upphovsrätt till litterära och konstnärliga verk" [Law about copyright to literary and artistic works]. http://62.95.69.3/SFSdoc/08/081416.PDF.

The Copyright Law, amended through SFS 2008:1416 Lag om ändring i lagen (1960:729) om upphovsrätt till litterära och konstnärliga verk (Changes to the law on copyright to literary and artistic works) affords protection to computer programs. The changing information technology environment has encouraged Sweden to tighten its copyright laws.

SFS 1998:112 Lag. "Om ansvar för elektroniska anslagstavlor, or BBS-lagen" [Law about the responsibility for electronic bulletin boards]. Amended through SFS 2005:315. http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=1998:112.

Outlines the Webmaster's responsibility to remove from electronic bulletin boards incendiary content, hate speech, child pornography, illegal violence, and material violating copyright.

SFS 1998:204. "Personuppgiftslagen/PUL" [Personal Data Act]. Amended through Lag (2008:187) om ändring i personuppgiftslagen [Law changing the Personal Data Act]. Information on the Personal Data Act, Ministry of Justice, 2006. http://www.riksdagen.se/ Webbnav/index.aspx?nid=3911&bet=1998:204.

Law covering personal identity protection.

SFS 2006:24 Lag. "Om nationella toppdomäner för Sverige på Internet" [Laws on major national domains for Sweden on the Internet]. http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2006:24.

SFS 2006:25 "Förordning om nationella toppdomäner för Sverige på" [Internet agreement regarding the use and security of such major Internet domain names as, e.g., "se."]. http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2006:25.

SFS 2007:213. "Lag om ändring i brottsbalken" [Law changing the Penal Code]. http://62.95.69.3/SFSdoc/07/070213.PDF.

Amends the Swedish Penal Code to include specific definitions of wrongdoing and punishment for illegal activity in the computer environment. This is in keeping with the European Union approach. See also "Angrepp mot informationssystem" [Attacks against the information system]. Proposed Government Bill 2006/07:66. http://www.regeringen.se/content/1/c6/07/86/73/af043821.pdf.

SFS 2007:951. "Förordning med instruktion för Post- och telestyrelsen" [Enactment with instructions for the Post and Telecom Agency]. http://www.riksdagen.se/webbnav/index.aspx?nid=3911&bet=2007:951.

Requires the Swedish Post and Telecom Agency to work for an effective and secure physical information technology infrastructure and to prevent information technology incidents.

SFS 2008:1002. "Förordning med instruktion för Myndigheten för samhällsskydd och beredskap" [Enactment with instructions for the Swedish Civil Contingencies Agency]. http://www. notisum.se/rnp/sls/fakta/a0081002.htm.

Instructs the Swedish Civil Contingencies Agency/Myndigheten för samhällsskydd och beredskap (MSB) to protect information security.

Swedish Government Agencies

A number of Swedish government agencies have information security responsibilities. The Swedish ministry responsible for information technology is the Ministry of Enterprise, Energy, and Communications (Näringsdepartementet). This ministry oversees the National Post and Telecom Agency (Post- och telestyrelsen), whose policy area includes electronic communications, information technology and postal communications, cashier services, and the emergency telephone service.

Several agency reorganizations and changes have transpired in the last few years. The relationship of these changes to Sweden's fight against cybercrime is uncertain. According to "Översikt av organisation av det nationella informationssäkerhetsarbetet" [Summary of national information security work], 2008, other agencies with information technology responsibilities include the following. However, this is by no means a comprehensive list of all the Swedish organizations involved in information technology security.

- Swedish Defence Matériel Administration (Försvarets materielverk). http://www.fmv.se.
- National Defence Radio Establishment (Försvarets radioanstalt). http://www.fra.se.
- Swedish Armed Forces (Försvarsmakten). http://www.mil.se.

- Swedish Emergency Management Agency—SEMA (Krisberedskapsmyndigheten—KBM). As of 2009, the Swedish Civil Contingencies Agency (Myndigheten för samhällskydd och beredskap—MSB) has absorbed SEMA, including the Swedish Emergency Management Agency's information security board (Krisberedskaps-myndighetens informationssäkerhetsråd). http://www.msbmyndigheten.se.
- Swedish Police Service (Rikspolisstyrelsen). http://www.polisen.se.
- Swedish Administrative Development Agency (Verket för förvaltningsutveckling—Verva). As of December 31, 2008, this agency is defunct, and information technology purchase activities are the responsibility of the Legal, Financial, and Administrative Services Agency (Kammarkollegiet). http://www.kammarkollegiet.se.
- Swedish Collaborative Group for Information Security (Samverkansgruppen för informationssäkerhet—SAMFI). This group includes the Swedish Defence Materiel Administration, the National Defence Radio Establishment, the Swedish Armed Forces, the Swedish Civil Contingencies Agency, the Swedish Police Service, the Swedish Information Technology Incident Center (Sitic), and the former Swedish Administrative Development Agency. http://www.sitic.se/samarbetspartners/ samverkansgruppen-foer-informationssaekerhet-samfi.
- Data Inspection Board (Datainspektionen). http://www.datainspektionen.se.
- National Security Administration (Regeringskansliet). http://www.ud.se.
- National Telecommunications Coordination Group (Nationella Telesamverkansgruppen—NTSG). http://www.pts.se/upload/Faktablad/En/facts-about-ntsg.pdf.
- National network for information and information technology security (Statligt nätverk för informations- och IT-säkerhet).
- Confederation of Swedish Enterprise (Svenskt Näringsliv). http://www.svensktnaringsliv.se and http://www.regeringen.se/sb/d/5291/a/101489.

As of 2009, Sweden has consolidated the Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap—MSB), the Swedish Rescue Services Agency (Räddningsverket), the Swedish Emergency Management Agency—SEMA (Krisberedskapsmyndigheten—KBM),[3] and the Swedish National Board of Psychological Defence (Styrelsen för psykologiskt försvar) into a new authority: Swedish Civil Contingencies Agency (Myndigheten för samhällsskydd och beredskap—MSB).[4] This authority now provides the cybercrime literature published by the previous entities.

The Swedish Standards Council (Sveriges Standardiseringsråd—SSR) has recognized the following as standards agencies in Sweden:

[3] Krisberedskapsmyndigheten (KBM) [Swedish Emergency Management Agency (SEMA)], http://www.krisberedskapsmyndigheten.se.

[4] Myndigheten för samhällsskydd och beredskap (MSB) [Swedish Civil Contingencies Agency], http://www.msbmyndigheten.se.

- Information technology standardization for telecommunications (Informationstekniska standardiseringen—ITS). http://www.its.se.
- Standardization in the area of electricity (Svensk Elstandard—SEK). http://www.elstandard.se.
- Swedish Standards Institute (Standardiseringskommissionen I Sverige—SIS). http://www.sis.se.

Swedish Standards Institute [Standardiseringskommissionen I Sverige (SIS)]. "Informationsteknik—Säkerhetstekniker—Riktlinjer för styrning av informationssäkerhet [Information technology—security techniques—guidelines for controlling information security]." ISO/IEC 17799, 2005, and Cor 1:2007, IDT, SIS, Stockholm, 2007. http://www.sis.se/DesktopDefault.aspx?tabName=@DocType_1&Doc_ID=40423&PresID=1&Desc=SS-ISO/IEC%2027002:2005.

The document reports standards in the ISO 27000 series, which provide guidelines for approaches to information security, such as the command system LIS. The ISO 27000 series updates the standard SS-ISO/IEC 17799:2005. These standards relate to information technology, security techniques, and guidelines for controlling information security.

Syrén, Agneta. *På egen risk: en handbok om informationssäkerhet* [At your own risk: an information security manual]. SIS series HB, Stockholm, 2005. http://www.sis.se/PDF/K_pguide_informationss_kerhet.pdf.

The manual explains the standard for information security SS-ISO/IEC 17799. The standard addresses new information security threats and risks. Good information security is an investment for all enterprises, and the manual provides practical guidance for assessing risk levels, cost-benefit analyses, relevant statistics, and goal setting. The manual refers to and complements the standards "Ledningssystem för informationssäkerhet" [Management systems for information security] SS 627799-2 and "Vägledning för styrning av informationssäkerhet" [Guidance for information security control] SS-ISO 17799.

Syrén, Agneta. *Stora säkerhetshandboken—En praktisk årskalender* [The big security manual—a practical calendar]. SIS HB 332, Stockholm, 2008. http://www.sis.se/DesktopDefault.aspx?tabName=@DocType_98&Doc_ID=67903.

Provides further security information in calendar format.