Copyright © 2017 International Journal of Criminal Justice Sciences (IJCJS) – Official Journal of the South Asian Society of Criminology and Victimology (SASCV) - Publisher & Editor-in-Chief – K. Jaishankar ISSN: 0973-5089 July – December 2017. Vol. 12 (2): 196–207. DOI: 10.5281/zenodo.1034658 / IJCJS is a Diamond Open Access (Authors / Readers No Pay Journal).

Cyber Crime and Legal Countermeasures: A Historical Analysis

Johannes Xingan Li[1]
Tallinn University, Estonia

Abstract

This article reviews the historical development of cyber crime and legal countermeasures. The article divides the process into four stages and concludes that cyber criminal phenomena have developed almost synchronously with Information and Communication Technology (ICT). Cyber crimes are in a process of accelerating development and are becoming gradually routinized. Notably, the electronic divide thus results in cyber crime divide. The basic conclusion is that criminal resources decide the amount of crime, while judicial resources decide the deterrence. When the balance is reached between criminal resources and judicial resources in the long term, the criminal phenomena will be saturated at an equilibrium point.

Keywords: Cyber crime, History, Deterrence, Legislation, Law enforcement, Criminal justice, Social control.

Introduction

The computer was an invention that people could not imagine until it was clear what it happened to be. Before the digital computer had been invented, Thomas Watson, the former chairperson of IBM predicted in 1943 "I think there is a world market for maybe five computers." Although different answers to questions "what exactly is a computer?" and "how many generations of computers have been developed?" are still running parallel, it is widely accepted that the first electronic digital computer was invented in the 1940s, in the final years of World War II (Hamilton, 1973, p. 82). The more notable example is the Electronic Numerical Integrator and Computer (ENIAC), invented in the U.S. in 1946 and since then, computer technology has experienced several generations.

Along with the continuous development of information technology, computer crime may, in principle, have been taking place since the very invention of the computer, but at that time, it neither became a significant problem nor caused great concern. Meanwhile, the development of computer crime should have kept pace with computer technology. The computer developed from a calculator to a word processor to a multimedia device. Besides the research on the history of ICT (Cortada, 2002), the history of the computer (Allan, 2001; Kuck, 1978, pp. 52-72); the history of the Internet (Okin, 2004) or of online information services (Bourne & Hahn 2004), and history of computer ethics (Bynum, 2001), scholars have also explored the history of cyber crime (Overill, 1998), and

[1] Associate Professor of International Law, School of Governance, Law and Society, Tallinn University, Tallinn, Estonia. E-mail: xingan.li@tlu.ee

particularly, the history of the hacker (Thomas, 2002; Peterson, 2003; Raymond, 2001, covering 1945 to 1990s), or the viruses (Dvorak & Pirillo, 2004). Some scholars have researched into the history of the legislation on cyber crime. Sieber (1996), for example, concluded that countries have adopted various forms of legislation, and undergone several waves from the 1970s, addressing different problems respectively. They provide a valuable foundation for analysis in this book. The different focuses in these researches do not deliberately furnish any organic links between the development of cyber crime and the development of deterrence. Yet these links are denoted as the primary concern of this article. Dealing with cyber crime, there proved to be multi-dimensional obstacles (Li, 2008), this article will present a retrospect of the history of cyber crime and relevant legislative and judicial practices.

Cyber criminal phenomena and the deterrence of punishment through law enforcement and social prevention are undergoing a process of development. The history of cyber crime can roughly be divided into four stages: a stage of germination, a stage of rapid development, a stage of broad expansion, and a stage of routinization. Furthermore, the criminal-law reform relating to cyber crime has never been completely synchronous with cyber crime due to a hysteresis in both the law enforcement and legislation compared with the relevant criminal phenomena.

Computer Hackers' Discovery of a Lawless New Frontier

Upon the hypothesis that computer crime emerged soon after the invention of the first computers, the first stage of computer crime began from the late 1940s and lasted through the late 1960s, when the general public paid more attention to usability, utility, efficiency, and development of the computer, and considered that the computer system was "occasionally unreliable," but "usually secure" (Dunlop & Kling, 1991, p. 524). Unlike today's universal use of computers, there was hardly a computer "market" in this early stage. The manufacture or installation of a computer is an expensive and time-consuming work. However, during this stage, computer crime emerged in the context of a limited number of computers in use, but the legislature did not provide any specific countermeasures against the phenomenon, leaving law enforcement to deal with it within the traditional legal framework.

Earlier studies implied that electronic computer" crime most probably emerged in the fields of military, engineering, science, finance and commerce at the beginning of the 1950s. Nevertheless, the earliest documented computer abuse, which involved the alteration of bank records, occurred in 1958 (Parker 1989, p. 5). The case became the first federally prosecuted computer crime in the U. S. in 1966, with a time-lag of eight years. It was revealed that a bank employee had utilized the institution's computer to embezzle cents from interest on long-term accounts (ibid.). The financially motivated employee created a criminal precedent.

Within less than two decades, worldwide computer installations increased from four hundred at the beginning of the 1950s to 60,000 at the end of the 1960s (Hamilton, 1973, p. 82). Even so, the scarcity of the new machine still attracted potential users to hack, to gain access, and to utilize unauthorized computer time. The term "hacker" in the traditional sense was not regarded as computer crime, but as essentially pertaining to computer security. The rise of the hacker culture can be dated to 1961 when the Massachusetts Institute of Technology acquired the first computer used for commercial time-sharing (Digital Equipment Corporation (DEC), Programme Data Processor-1, 1963). The expensiveness and rareness of computers necessitated a shared use of these machines to extend their utility as widely as possible, in which the boundary between authorized and unauthorized use was vague. However, at the same time, a security concern originated due to the breach of access control (Association for Computing Machinery Professional Knowledge Programme, 1997). The exploited processing ability, loss of computing time and even waste of electricity alarmed computer owners. Notwithstanding, the computer systems were not generally confronted with threats as serious as the phone systems were. In consequence, the U. S. took action to prevent tampering with the phone system (Meinel, 2004). Being an early form of hackers, phreakers' intrusion into and interference with the telecommunications system became a kind of punishable offence.

War has been the perpetual inventor in history. Although the apparent causal relation between the Cold War and the ARPANET was not widely acknowledged in available literature, the latter was surely a product to deal with the threats of a "Hot War" against data transmission system. The advantage of this invention was that even if one part of the system was destroyed by war, particularly by nuclear weapons, the system could function in its other parts through rerouting (Okin, 2004, particularly, p. 132). The Internet began in the mid-1960s as a programme created by the U. S. Department of Defence to build a decentralized network that would provide a communication between various sectors of the government in the event of nuclear war or an attack on the U. S. (Hafner & Lyon, 1998, pp. 10-14). The nature of the Internet determined that it was connected primarily to some important institutions, but was not open to the general users. An intrusion of the networks would endanger interests that were mainly military and those of advanced science and technology.

At the beginning of this first stage, there was neither cyber crime nor cyber criminal law in the social and legal environment. When the first computer crimes occurred, no law was ready to deal with them (Chen, 1990, pp. 71-86; Nelson, 1991, pp. 299-321). With the emergence of the cyber criminal phenomenon, the principle of "*nullum crimen, nulla poena sine lege*" was applied to protect the fundamental rights of the perpetrators from punishment outside the law. Except for the reluctant application of old laws, there was neither a cyber crime prohibited by law nor a law enacted against cyber crime. Lack of punishment reduced the expected cost of the criminals, which were composed thus of moral costs and substantial costs, specifically, the perpetrators' necessary devices and labour in cyber crime. Because there was no cyber crime law, there was neither expected punishment nor the expected cost induced by the expected punishment. Under such circumstances, the probability of conviction equalled zero. The expected utility of the perpetrator almost equalled the utility of a situation in which crime went undetected or unpunished. According to an economic analysis of crime (Becker 1968, pp. 169-217), those who are risk-indifferent are indifferent to detection and conviction. For those who are risk-lovers, cyber crime becomes a new cause, a new chance, a new challenge, and a new type of risk. For those who are risk avoiders, because of the low risk of detection and conviction rate of cyber crime, they transfer from other offences to cyber crime. Therefore, the number of cyber crimes and perpetrators will inevitably increase.

Apart from the gap in legislation when the first cyber crime emerged, law enforcement had insufficient capacity to deal with it. However, they tried towards imposing punishment through application of existing laws. This provided for a preliminary deterrence on cyber crime, which could be used to deter the potential offenders of existing types of crimes proscribed by existing laws, but was inadequate to deter potential offenders of the types of crimes not proscribed explicitly by law. The principle of legality and the limited possibility of the legislation restrained the coverage of the law and law enforcement, leaving considerable loopholes and having little deterrence on offences that remained untouched by law. As a result, deterrence brought very low expected costs for these perpetrators.

At the same time, existing laws were applied to the limited number of computer crime cases in countries such as the U. S. In filling the legal gap, the passage of computer crime legislation by states lagged behind computer abuses, and did not happen in this period. Furthermore, the debate about computers and personal information only began in the late 1960s (Wood 1982, p. 111). The debate did contribute to providing some forms of deterrence.

The Rise of the Law against the increasing number of Cyber Crimes

Following the first stage, the subsequent two decades form the second stage, which began from the 1970s and lasted to the end of the 1980s, during which along with individuals' and organizations' increasing dependence upon computers, the threats of computer crime increased. The general tendency was that computer crime continued to increase in volume with a change in methods, while a legal response also began to emerge.

Understanding of the nature of the computer continued developing. In a British case, R. v Wood, the court held that "The computer was used as a calculator, a tool which did not contribute to its own knowledge but merely carried out a sophisticated calculation which cannot have been done manually" (R. v Wood [1982] 767 Cr. App. Rep. 23.). It was not a rare situation that even many commentators doubted the acceptability of the computer, predicting only with extreme carefulness that: "The electronic computer would be technology's most successful machine were it not for the difficulty that people have in accepting it." (Hamilton, 1973, p. 81) Others already began to long for the "post-industrial society" (Bell, 1974), where the computer would not only be broadly used but also be addictively depended on.

Technological thought developed fast in changing the image of the computer in the 1970s, from a bulky mainframe that filled a building to a computer in a desk; and in the 1980s, from a desktop to a host of old and new devices (Mosco, 2004, p. 21). The focus of this philosophy is that: "The computer would be growing in power while withdrawing as a presence" (ibid.). The philosophical imagination and the technological development of new intelligent instruments were propelling an information revolution. Comparatively instant and cheap, an e-mail message could be sent from New York to San Francisco in less than a minute for about one dollar, as Fetherolf (1982, pp. 216-217) said. The futurist Castells bore witness to the fact that: "We are in the middle of a major technological revolution that is transforming our ways of producing, consuming, organizing, living, and dying" (Castells 1985, p. 11).

While technology advanced beyond the ability of the average citizens' understanding, (State ex rel. McCleary v. Roberts, 88 Ohio St.3d 365, 2000-Ohio-345.) the operation of computers remained straightforward and vulnerable to criminal manipulation (Bequai, 1979, p. 107). According to Bequai, computer crimes during this period fell into five key categories, specifically, vandalism, theft of information, theft of services, theft of property, and fraud (1979, pp. 106-107). Both the merely psychic satisfaction and the pecuniary gains motivated users to practise unauthorized access to the machines, or to information in the machine, hacking for use only being a less guilty act. In fact, before the 1970s, "using" computers without authorization was more excusable because the available computers were still insufficient. Later in the 1980s, more computers were available and it became unnecessary for general users to intrude into others' systems. Therefore, unauthorized "use" of computers no longer provided an excuse and became labelled "abuse" in legal terms.

During this period, there were only some fragmentary reports of computer abuses and accidents. However, the less bulky, low-cost computer attracted an unprecedented number of hackers with various motivations. Computer crime was comparatively new and authorities reacted in a sluggish manner. It was found that the threat of computer crime was pretty relentless. For instance, the average loss of computer crime was dozens or hundreds of times that of conventional crimes, regardless of whether the hackers obtained monetary benefits or psychological satisfaction.

Within this stage, the term "cyberspace," first coined in a fictional work by William Gibson (1984) to describe the environment within which computer hackers constructed a virtual community, became prevalent. In 1978, nevertheless, a perpetrator deprived a bank of 10.2 million dollars in the Rifkin case (Forester, 1990, p. 263). In 1982, a group of hackers intruded into a computer with records of cancer patients' radiation treatment, modification of which might threaten the lives of these patients. Murder became realistic with the computer as a tool (Milhorn, 2005, p. 59). In 1986, Stoll uncovered an international espionage conspiracy (Longstaff & co-workers, 1997, p. 234). These cases expressed again the potential threats of the hackers against property, life, and state security.

On the other hand, the development of computer technology, which was designed for social welfare, also constituted a significant source of threats to the social order. Similarly, the history of technology has been filled with dilemmas of such a kind. For example, primitive weapons may exactly be productive tools and vehicles may be hijacked. What was going to happen –unfortunately- in the field of computer science was that something destructive would be invented. For example, Dan Edwards coined the term "Trojan Horse" in 1972, denoting an apparently benign macro or utility with undocumented side effects, which may be security violating or palpably destructive (Overill, 1998). The Trojan horse caused great security anxiety with institutions such as the military (ibid).

Although it is not an exclusive argument, it has been broadly acknowledged that it was in 1984 when Fred Cohen defined a computer virus in his paper (1984). The threat of malicious programmes such as a Trojan Horse, a virus, a worm, and a logic bomb, all came into being during the 1980s, and necessitated the first business of anti-virus in 1988 (F-secure 2005). These soft offensive and defensive weapons were expected to play their roles in the information warfare in the near future.

The computer network still played a tiny role during this period. As Clarke (1984) pointed out: "Even for highly developed countries, these [data and computer networks] are still in their infancy, though they undoubtedly represent the wave of the future" (p. 27). Nevertheless, computer security incidents increased steadily with the development of computer networks. Losses due to computer crime had been incessantly escalating. In 1980, losses from computer fraud and other abuse of computer systems in the U. S. alone were estimated to exceed 300 million dollars (Wood, 1982, p. 69). In contrast, although software theft found its way in 1964 (Forester, 1990, p. 3), and in the late 1970s, large-scale piracy became common due to the use of the personal computer and packaged software (Forester, 1990, p. 4), there have been very few breaches of privacy reported (Wood, 1982, pp. 118-119.).

In the early 1970s, according to Sieber (1998), most developed countries introduced laws criminalizing computer crime. More laws and regulations were implemented in more countries in the 1980s. Within this period, all of the Nordic countries had their data-protection laws in place. Countries made every effort to eliminate legal gaps to punish cyber crime. The characteristics of legal countermeasures during this stage were that:

- There were merely fragmental computer crimes and fragmental legislations;
- Legislation concerning computer crime was generally concentrated in a developed country;
- New crimes such as time theft posed considerable contradictories in the field of law (BloomBecker, 1981, pp. 16-17);
- Laws were not effective enough (See Dierks, 1993, pp. 307-342; see also Rosenblatt, 1990, p. 35), and there was a general "lack of deterrence" (Bequai, 1978, pp. 5-6).

In short, at the second stage of the development of cyber crime and deterrence, cyber crime was in its growth period, with both the extent of cyber crime and the supply of perpetrators increasing. Although the costs of cyber crimes were continually increasing due to the increasing legislation and law enforcement, they were lower than other well-punished crimes. This is why rational criminal investors rushed into the new field. Countermeasures against the increasing crimes increased deterrence, which represented an increased probability of detection by new police forces and an increased severity of penalty through new laws. In the development of the struggle between cyber crime and punishment, most types of cyber crimes emerged and to a certain extent were deterred.

A Legal System Wrestling with Networked Adversaries

The pace of cyber crime became faster and faster. The third stage roughly covered the whole of the 1990s, when cyber crime expanded and the relevant legislation was broadly implemented. During this period, personal computers entered homes and offices throughout the developed world and even in the less-developed countries (Mosco, 2004, p. 2). Bill Gates,' *The Road Ahead* (1995), Nicholas Negroponte's, *Being Digital* (1995) all concentrated on building a new world in cyberspace. Tapscott (1996) announced that: "Today, we are witnessing the early turbulent days of a revolution...A new medium of human communications is emerging, one that may prove able to surpass all previous revolutions...in its impact on our economic and social life" (p. xiii).

Although the information revolution was processing with different styles in countries at a different economic level, the impact of computers on society seemed to be reaching into every aspect of social life (Mosco, 2004, p. 18). Alongside the scientists who were hopeful of the new development, the politicians in addition attempted to connect computer communication, economic growth, democracy, and a better environment. As Al Gore said: "…[W]e will derive robust and sustainable economic progress, strong democracies, better solutions to global and local environmental challenges, improved health care, and…a greater sense of shared stewardship of our small planet" (Gore 2004).

However, since the 1990s, cyber crime had entered a rapid process of globalization. Initially funded by the government, and limited to academic and official uses, the interest in the commercial use of the Internet began to be satisfied from the early 1990s; since then, computer networks have attracted great public attention (Kollock & Smith, 1999, p. 3). The U. S. introduced the concept of the National Information Infrastructure (NII) to "unleash an information revolution" (Rowland, 1998). With the invention of the WWW, access to the Internet was available to average users. The growth of the Internet was surprisingly fast. From then on, global computers connected to and users acquiring access to, the Internet were confronted with threats from a globalized cyberspace. Following the last stage, cyber crimes have developed into forms that are more complicated. The cyberspace where perpetrators lived, the virtuality that they wanted, the cable by which they were linked, the knowledge that they had acquired, the tools that they invented, and the platform on which they shared information provided criminals of different degree of sophistication with new incentives.

Personal information could be caught during the transmission process. Personal computers could be attacked during voluntary surfing of the Internet. Web sites could not only be tools by which attacks were carried out, but could also be targets for attacks. According to the statistics by Alldas.de, about 72 web sites were defaced by 47 attackers in 1998, about 1,079 web sites defaced by 430 attackers in 1999 (Li, 2003). The General Accounting Office reported 250,000 attacks against the U. S. Department of Defence computers in 1995. These numbers represented different aspects of the situation of risks and threats on the Internet.

Cyber criminals also found their way into electronic communications, such as the e-mail, the abuse of which became an advertising means for underground marketing, or an annoying forum. The large-scale unsolicited e-mail became known as spam (Kelly, 2002), which has been converted into one of the side products of electronic marketing.

Moreover, a series of attacks from malicious programmes happened (Drummond and McClendon 2001), and web sites suffered great threats. The businesses of anti-virus and of the security services continued developing. By 1990, many anti-virus products were introduced from big companies. To some extent, this indicated that the security-induced cost of individual and organizational users had further increased.

The victimized entities began to report enormous losses caused by the infringement of intellectual property. Many web sites, software authors and ordinary Internet users adopted various ways of transferring and exchanging pirated works. The infringement of copyright text, audio, video and multi-media works had entered a stage that seemed impossible for any of the existing authorities to control.

Cyber criminals attacked various private and public targets all over the world, in respect of which some hacking investigations were successful in arresting the perpetrators. In the U. S., the FBI opened 547 cases of "computer intrusion" in 1998, while the number of such cases increased up to 1,154 in 1999 (Freeh, 2000). The financial crisis in Asia and a series of bankruptcies of big enterprises also alerted attention to the fact that cyber crime could bring about disasters to the global economy.

Starting from this period, with the rapid rise of the Internet, the influence of the Internet on cyber crime began to be considered in legislation, the contents of which became rich and the range of which was expanded. The gradual formation of international harmonization affected some national legislation. Computer crime and relevant legislation was globalized, expanded from developed countries to less developed countries and to developing countries. Law enforcement also took a series of measures against cyber crime.

For example, in 1990, the U. S. organized a nationwide crackdown on cyber crime, leading to successful arrests, criminal charges, a dramatic show-trial, a number of guilty pleas, and massive confiscations of digital evidence and equipment (Sterling, 1994).

From the above analysis, it can be found that at the third stage of development, cyber crime tended to be saturated and the growth rate was thus decreasing. To reach this stage, most types of cyber crimes emerged and been criminalized, the probability of detection had reached a higher level, severity of punishment had reached a higher degree, and most potential users of computers and networks were connected, leaving little space for the undeterred types of cyber crime. The marginal benefits of one more case of cyber crime was going to decrease, while the marginal costs of one more case of cyber crime was going to increase (for general theory about marginal costs and marginal benefits of crime, see Becker 1968; for modern application of this theory, see Cooter & Ulen, 2003). Therefore, cyber crime tends was being saturated. At this stage, deterrence continued to increase to a certain extent, until it reached the completeness, specifically, the optimality of marginal utility.

The Equilibrium between Cyber Crime and Deterrence

Although the commencement of the year 2000 witnessed a surprising breakdown in the network economy boom (Mosco, 2004, p. 45), the cyber criminals did not demonstrate any sympathy with the dot coms nor with the stock markets. The fourth stage developed roughly from the year 2000, when cyber crime was becoming routinized, and the legal gap filled.

The large-scale Denial of Service attack against high profile web sites created great panic in society about the Internet infrastructure (Levinson, 2002, pp. 524-525). A long list of viruses that were written by people who were in jurisdictions where there was no law against hacking, that were written by means of specific software, which included multiple methods of attacking, that caused billions of dollars of losses, and that disabled anti-virus products, indicated the seriousness of the threat and the necessity for the countermeasures (See Katyal 2001, pp. 1003-1114).

In contrast to these anarchist attacks, the advance-fee fraud induced the victims to transfer money voluntarily to the criminals. The advance-fee fraud, or 419 fraud, which was named after the applicable section of the Nigerian criminal code and was committed in a more organized manner, has victimized people from around the globe. The average Nigeria 419 victim has lost 5,575 dollars, making 419 fraud one of the most costly financial frauds for individuals (Fager, 2004, p. 20).

As to the increase of web sites, attacks against web sites rapidly increased. According to the statistics of Alldas.de, about 4,394 web sites were defaced by 2,255 attackers in 2000, while about 4,797 web sites were defaced by 667 attackers in the first season of 2001 (Li, 2003). The defacement of web sites became a significant problem comparable with graffiti street buildings.

The quantity of cyber crime incidents and malevolent attacks has, nevertheless, fallen from year to year since 2001. According to a survey conducted by the CSI and the FBI in 2003, general financial losses totalled, from 530 survey respondents, 201.7 million dollars, a sharp drop from the previous survey total of 455.8 million dollars. In the 2004 survey, overall pecuniary losses totalled, from 494 survey respondents, 141.5 million dollars (CSI, 2004). In 2005, the survey indicated losses, from 639 respondents, that totalled 130.1 million dollars (CSI, 2005, p. 14). In recent years, the tendency of decreasing remains

(CSI, 2011, p. 11). The reasons for these reduced figures were not clear, but the improved security measures, law enforcement, legislation and international cooperation may all contribute to prevent cyber crime. Of course, at the same time, we can see that there could be fluctuations over the years, like the development of traditional crimes.

Many developed and developing countries have implemented cyber crime laws. From the point of view of International harmonization, the Convention on Cyber crime entered into effect on 1 July 2004. Starting from the 9/11 attacks, a serious international concern about cyber terrorism was brought about the by large-scale distributed denial of service attacks, and it spread among governments, legislatures, law enforcements, and academia.

At the fourth stage, due to the decrease in the marginal utility and increase of the marginal cost of one more crime, and the constant increase in the means of deterrence, total number of cyber crimes has shown a prospect of decrease in so far as the potential perpetrator realizes the fall in the optimality of benefit from cyber crime (for general theory about marginal costs and marginal benefits of crime, see Becker 1968; for modern application of this theory, see Cooter & Ulen, 2003. For a study on economic analysis of cyber crime, see Li, 2005). The cyber criminal will, additionally, have to take higher risks than before. It turns out that risk-avoiders will retreat from cyber crime, that those who are risk-neutral and risk-lovers will also discover it less attractive to commit cyber crime than other crimes, and tend to discontinue their adventure. Under such circumstances, the deterrence exercised by legislation and law enforcement can ultimately be recovered.

Conclusion

During recent decades, society has experienced a fast and frightening increase in both information and communications systems and information transgression. The development of cyber crime follows a route of innovation of the ICT, generations of computers, enlargement of the networks and emergence of anti-security techniques. The faster the speed of information processing is, the broader the network connection covers, the more users are engaged in the information industry, and the more dependent on information modern society becomes, the higher the risks and the more serious the threats people will have to face. Naturally, the number and gravity of cyber crime will also increase. However, any increase will not be limitless.

The basic summary of the historical scene revolving around cyber criminal phenomena presents us with the reality that the increase of both cyber crime and deterrence remain unbalanced. In a word, people do much, but not enough.

References

Allan, R. A. (2001). *A History of the Personal Computer: The People and the Technology*. London, Ontario: Allan Publishing.

Association for Computing Machinery. (1997). *Professional Knowledge Programme*. New York, NY: Association for Computing Machinery.

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy*, 76, 169-217.

Bell, D. (1974). *The Coming of the Post-Industrial Society*. London: Heinemann.

Bequai, A. (1978). *Computer Crime*. Lexington, Massachusetts, Toronto: Lexington Books.

Bequai, A. (1979). *White-Collar Crime: A 20th Century Crisis*. Lexington, Massachusetts: Lexington Books.

BloomBecker, J. (3 August 1981). Employee Computer Abuse –What to Do?. *The Los Angeles Daily Journal*, pp. 16-17.

Bourne, C. P., & Hahn, T. B. (2004). *A History of Online Information Services, 1963-1976.* Massachusetts: Massachusetts Institute of Technology Press.

Bynum, T. (2001). Computer Ethics: Basic Concepts and Historical Overview, in Stanford Encyclopaedia of Philosophy. Retrieved from http://plato.stanford.edu/entries/ethics-computer.

Castells, M. (1985). High Technology, Economic Restructuring, and the Urban-Regional Process in the United States. In M. Castells. (ed.). *High Technology, Space, and Society* (pp. 11-40), Urban Affairs Annual Reviews, volume 28, Beverly Hills, London: Sage Publications.

Chen, C. D. (1990). Computer Crime and the Computer Fraud and Abuse Act of 1986. *Computer Law Journal*, *10*(1), 71-86.

Clarke, A. C. (1997). *3001: The Final Odyssey*. Hammersmith, London: Voyager.

Clarke, A. C. (1984). *1984: Spring*, London: Granada Publishing.

Cohen, F. (1984). Computer Viruses-Theory and Experiments, IFIP TC 11 Conference, Toronto. Retrieved from http://www.all.net/books/virus/index.html.

Cooter, R., & Ulen, T. (2003). Law and Economics, fourth edition, Addison Wesley, 2003.

Cortada, J. W. (2002). *Making the Information Society: Experiences, Consequences, and Possibilities*, Englewood Cliffs, New Jersey: Prentice Hall PTR.

CSI. 2004. CSI/FBI (2004). Computer Crime and Security Survey.

CSI. 2005. CSI/FBI (2005). Computer Crime and Security Survey.

CSI. 2011. CSI/FBI (2011). Computer Crime and Security Survey, p. 11.

Dierks, M. P. (1993). Computer Network Abuse. *Harvard Journal of Law and Technology*, *6*, 307-342.

Drummond, N., & McClendon, D. J. (2001). Cybercrime- Alternative Models for Dealing with Unauthorized Use and Abuse of Computer Networks. Retrieved from http://gsulaw.gsu.edu/lawand/papers/su01/drummond_mcclendon.

Dunlop, C., & Kling, R. (1991). Introduction to Security and Reliability. In C. Dunlop & R. Kling (eds.), *Computerization and Controversy: Value Conflicts and Social Choices* (pp. 524-532). San Diego: Academic Press.

Dunlop, C., & Kling, R. (eds.). (1991). *Computerization and Controversy: Value Conflicts and Social Choices*. San Diego: Academic Press.

Dvorak, J. C., & Pirillo, C. (2004). *Online!* Pearson Education.

Fager, C. (9 December 2004). The 419 Fraud. *Christianity Today*, *46*(13), 20.

Fetherolf S. (1982). Telecommunications and the Future. In H. F. Didsbury (ed.) *Communications and the Future,* (pp. 211-222). Chicago: World Future Society.

Forester, T. (1990). Software Theft and the Problem of Intellectual Property Rights. Computer and Society. 20(1), 2-11.

Freeh, L. J. (28 March 2000). Statement for the Record of Louis J. Freeh, Director FBI on Cybercrime Before the Senate Committee (Judiciary Subcommittee for the Technology, Terrorism, and Government Information), Washington, D.C. Retrieved from http://www.cybercrime.gov/freeh328.htm.

F-Secure. (2005). F-Secure Expands Asian Business and Launches First Major Internet Service Provider Relationship. Retrieved from http://www.f-secure.com/news/items/news_2005092800.shtml.

Gibson, W. (1984). *Neuromancer.* New York: Ace Books.

Gore, A. (21 March 2004). Speech to the International Telecommunications Development Conference, Buenos Aires.

Hafner, K., & Lyon, M. (1998). When Wizards Stay up Late: The Origins of the Internet (pp. 10-14). New York: Simon and Schuster.

Hamilton, D. (1973). *Technology, Man and the Environment.* London: Faber and Faber.

Katyal, N. K. (2001). Criminal Law in Cyberspace. *University of Pennsylvania Law Review, 149*, 1003-1114.

Kelly, J. X. 2002. Cybercrime - High Tech Crime, JISC Legal Information Service - University of Strathclyde. Retrieved 15 June 2016, from http://www.jisc.ac.uk/legal/index.cfm?name=lis_cybercrime

Kollock, P., & Smith, M. (1999). Communities in Cyberspace. In: M. Smith & P. Kollock (eds.), *Communities in Cyberspace* (pp. 3-28). London: Routledge.

Kuck, D. J. (1978). *The Structure of Computers and Computations.* New York: John Wiley and Sons.

Levinson, D. (ed.). (2002). *Encyclopedia of Crime and Punishment.* Newbury Park, CA: Sage Publications.

Li, X. (2003). Lun Wangluo Fanzui (Crimes on the Internet), Law Library. Retrieved from http://www.law-lib.net/lw.

Li, X. (2005). Economic analysis of cybercrime: the mixed provision of private goods. In: J. Roufagalas (Ed.), *Resource Allocation and Institutions: Explorations in Economics, Finance and Law* (pp. 607−620). Athens, Greece: ATINER.

Li, X. (2008). *Cyber crime and Deterrence: Networking Legal Systems in the Networked Information Society*. Turku: Uniprint.

Longstaff, T. A., & co-workers. (1997). Security of the Internet, in The Froehlich/Kent Encyclopedia of Telecommunications. *15*, 231-255. New York: Marcel Dekker.

Meinel, C. (2004). *Computer Hacking--Where Did It Begin and How Did It Grow? Guide to Harmless Hacking*. Beginners' Series, 5.

Milhorn, H. T. (2005). *Crime: Computer Viruses to Twin Towers.* Boca Raton, Florida: Universal Publishers.

Mosco, V. (2004). *The Digital Sublime: Myth, Power, and Cyberspace.* Massachusetts: The MIT Press.

Nelson, B. (1991). Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm. *Computer Law Journal*, 11(2), 299-321.

Okin, J. R. (2004). *The Internet Revolution: The Not-for-dummies Guide to the History, Technology, and Use of the Internet.* Winter Harbor: Ironbound Press.

Overill, R. E. (1998). Computer crime - An Historical Survey. Retrieved from http://www.kcl.ac.uk/orgs/icsa/Old/crime.html.

Parker, D. B. (1989). *Computer Crime: Criminal Justice Resources Manual.* National Institute of Justice.

Peterson, T. F. (2003). *Nightwork: A History of Hackers and Pranks at MIT.* Massachusetts: Massachusetts Institute of Technology Press.

Raymond, E. S. (2001). *The Cathedral and the Bazaar*. Sebastopol, California: O'Reilly and Associates.

Rosenberg. M. J. (2001). E-Learning: Strategies for Delivering Knowledge in the Digital Age. New York: McGraw-Hill.

Rowland, D. (1998). Cyberspace - A Contemporary Utopia? *The Journal of Information, Law and Technology*, 1998, number 3. Retrieved from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/rowland.

Sieber, U. (1996). Computer Crime and Criminal Information Law - New Trends in the International Risk and Information Society - Statement for the Hearing on Security in Cyberspace of the United States Senate, Permanent Subcommittee on Investigations, Committee on Governmental Affairs, 16 July.

Sieber, U. (1998). Legal Aspects of Computer-Related Crime in the Information Society, The COMCRIME-Study for the European Commission. Retrieved from http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html.

Sterling, B. (1994). The Hacker Crackdown: Law and Disorder on the Electronic Frontier, Austin, Texas: Electronic Release. Retrieved from http://www.gutenberg.org/dirs/etext94/hack12.txt.

Tapscott, D. (1996). *The Digital Economy: Promise and Peril in The Age of Networked Intelligence*. New York: McGraw-Hill.

Thomas, D. (2002). *Hacker Culture*, Minneapolis, Minnesota: The University of Minnesota Press.

Wood, M. B. (1982). *Introducing Computer Security*. The U.S.: NCC Publications.