Scientific and Practical Cyber Security Journal (SPCSJ) 2(2):38-58
Scientific Cyber Security Association (SCSA), 2018 ISSN: 2587-4667

VULNERABILITIES OF THE WEB: A SOCIO-LEGAL VIEW

Xingan Li
International Institute for Innovation Society, Helsinki, Finland

ABSTRACT

The purpose of this article is to review the social-legal environment of the emergence of cybercrime. The pervasiveness of information and communications systems brings about a legal gap in regulating the new crimes and new forms of existing crimes. There is also the inevitability for extending the objects that the criminal law should provide shield. The swift progression of technology and the inactivity of legal instruments form a sharp contrast. The multiple roles of computer systems in crime, and the decentralization of the Internet make it more complicated to combat cybercrime effectively through any single measure.

KEYWORDS: Networked society; Universal accessibility; Uncontrollability; Invisibility; Disputability; Divisibility; Low confidentiality; Anonymity; Abuse; Uncertainty of the future

Information and communications systems are producer, container, processor, and transmitter of information. The Internet bears an identity of technological creation and technological concept, under which the connection of computers forms a network, while the congregation of networks forms the Internet (Forcier and Descy 2002, pp. 40-60), being borderless and decentralized, and connecting global computers by Hypertext Transfer Protocol (HTTP). The Internet is merely a wide-reaching congregation of computer networks supported by Internet technology, providing possibilities of mutual communications and of access to information.[1] It does, therefore, not only link machines, but also more importantly "links people, institutions, corporations and governments around the world."[2] Each of the services that the Internet makes available may possibly bring about legal problems, increasing opportunities of cybercrime (Grabosky 2000, pp. 2-3.)

Although countless statistics and empirical studies have tried to depict the development of the Internet, this paper tries to present an illustration of the Internet through such aspects as the increase of Internet users, web sites, Internet hosts, web pages, bandwidth, and the growth of e-commerce. The term "indicator" is used to denote these factors in describing the size of the Internet.

The first indicator is the number of personal computers (PCs) and the Internet users. The scale at which information technology has influenced society can roughly be measured by the proportion of the population with access to computers and the Internet. The primary function of information and communications systems is to process and share information.[3] The more the computers are manufactured, traded and used, to a higher extent will society depend on this intelligent machine. The more the people are connected to the Internet, the greater the share information and communications systems-mediated telecommunications will have for the entire market. In no easy

[1] Reno v. American Civil Liberties Union, Supreme Court No. 96-511, 26 June 1997.
[2] American Civil Liberties Union v. Johnson (Tenth Circuit No. 98-2199, November 1999).
[3] Panavision Intl. v. Toeppen, Ninth Circuit No. 97-55467, D. C. No. CV-96-03284-DDP, 17 April 1998.

way can we count personal computers in use globally, but according to the International Telecommunications Union, up to 2004, there were approximately 772 million personal computers in use in the world (GeoHive 2006). It means that practically thirteen percent of the world population are PC users (ibid.). While the Internet has expanded into 214 countries and world regions, the worldwide Internet users have been increasing fast in the past ten years. in 2007, the global networks of information and communications systems have connected approximately 1.15 billion people (Internetworldstats.com 2007), while in 2015, the number is nearly tripled and reached 3.27 billion (Internetworldstats.com 2015). In 2007, more than one-fourth of them are online Europeans, who have the penetration rate of 39.8 percent (Ibid). In the European Union alone, the 255.58 million Internet users represent an average of more than half the whole population in these countries (Internetworldstats.com 2007). Today, users in Asia constitute nearly half of world Internet population (Internetworldstats.com 2015). The number of European users falls into not more than one fifth (Ibid.). The overall number of world Internet users increased eightfold (Ibid).

As one of the fast increasing fields, Social Networking Services (SNSs) spread in a surprising rhythm into contemporary social life. While the number of users of the SNSs is not available, it was estimated that among Internet users, about 74% of online adults use social networking sites (Pew Research Center 2015). In fact, at present, SNSs are used in a broad range of mobile devices, such as smart phones, cameras, media players, tablets and phablets, and notebook PCs, which are usually connected to the networks when they are in use.

The number of Internet users has a high referential value in measuring the importance of cybersecurity, and the harmfulness of cybercrime. The increase in the number of users represents a transition from non-PC-users to PC users, from non-Internet-users to Internet users, which in turn represents a transition from a lower likelihood of being informed to a higher likelihood of being informed—informed by information of various value orientations: coincident with inherent value notion, or contradictory to it. Problems emerge during the process of personal changes to PC usage caused by the subsequent access to more information and social changes as a result of its members’ access to ever-more information.

Suppose the total population constant, the users are fewer than non-users but increasing at a phenomenal rate, while the non-users are more than users but decreasing, a movement from non-users to users. I think of the process as a sandglass. The increase of users is like the flow of sand from the top bulb to the bottom bulb. As to what happens in the sandglass, conflict and crash are inevitable. So it is between users: old users and old users, old users and new users, new users and new users and actually between old users and non-users, and new users and non-users, and so forth. If we consider these users are in different organizational forms, it will become more complex: individual users versus corporate users, and so forth.

Users are not only the subjects in the maintenance of cyberspace order; they are among the potential victims of cybercrime. They may benefit from online activities, and at the same time, they may otherwise suffer losses when targeted by cybercriminals. The figure represents the growth of the online population, which is increasing by a surprising rate compared with population in the traditional society. The citizens in the traditional society do not decrease as the netizens in the cyberspace increase. However, more and more people are obtaining the dual identity as both citizens in society and netizens in the cyberspace.

The crime rate in cyberspace may be low at present. Suppose this rate constant, the absolute number of cybercrime, however, increases along with the growth of the population base of Internet users.[4] Consequently, the number of Internet users is valuable in the calculation of the number and even the rate of cybercrime, in comparison with those figures in traditional society.

On the other hand, given that cybercriminals are also among the Internet users, their growing number and their increasingly extensive geographical distribution indicate the difficulties in cyberspace regulation, cybercriminal detection, investigation, jurisdiction, identification, and conviction, and the costs and effectiveness in crime prevention. The Internet has been expanded to virtually all countries in the world. The Internet contents are using more and more kinds of languages, but with a relative concentration in some main languages, such as English, Chinese, Spanish, Japanese, German, French, Portuguese, Korean, Italian, and Arabic (Internetworldstats.com 2007). People understanding different languages will be more or less Internet-informed, but people who understand the main languages will be more Internet-informed. Therefore, the possible impact of online information on users who understand different languages differs. These numbers and ratios will be constructive in understanding the controllability of the Internet and thus the characteristics of cybercrime.

The second indicator is the increase in the number of web sites, which represents the number of cyber actors, the quantity of cyber resources, the range of services that users can consume, and the number of places that the potential customers can visit. A Netcraft survey in July 2006 found that there were more than 88.2 million web sites on the Internet.[5] From the increasing process of the Internet domain names worldwide, an accelerated ratio of increase can be discovered from the late 1990s.

The primary function of web sites is to serve the Internet users' needs of information resources. It is an important form of information publication, which acts as the counterpart to the traditional printed press. The growth of cyberspace population and the growth of web sites interact with each other. The users include publishers and readers, both of whom can exchange their status with each other. The growing number of web sites accommodates more users, while the growing number of users propels the development of web sites. It is possible that the criminals will be destructive towards the web sites, and in turn, that the users' interests will be damaged thereby. The web sites can also facilitate activities unsuitable for the participation of certain groups of people or the web sites may to publish content unsuitable for certain groups of people to retrieve. Lack of a unified conception concerning whether or not to monitor or censor the use of the Internet may leave this public forum in a status of anarchy and confusion.

In addition, the location of web sites is not the equivalent to in the traditional sense. A web site may exist in several regions or countries simultaneously, including at least in the following possible places:

The location of the web site registration,
The location of the web site owner,
The location of the web site server,
The location of the content author,

[4] Similarly, Parker and Nycum (1984, p. 314) estimated that the volume of computer crime would increase due to the growth in the number of computers.

[5] Netcraft. July 2006 Web Server Survey, 28 June 2006. Retrieved 15 March 2016, from http://news.netcraft.com/archives/web_server_survey.html

The location of the web site manager (webmaster),

The location of the web site retriever,

The location of where the language of the web site is mainly spoken by the native people,

The location of where the web site can mainly be accessed, and where the web site can have an actual influence, etc.

Determination of jurisdiction and harmonization of legislations are based significantly upon these different kinds of locations. The simultaneous involvement of many locations in a single act makes it difficult to select a certain location as the nexus for jurisdiction. The involvement of more locations during the process of information transmission and the complexity of tracing backward pose obstacles for determining the just location. Information and communications systems become an information high sea full of information flow.

The third indicator is the number of Internet hosts. An Internet host denotes a computer connected directly to the Internet; regularly, an Internet Service Provider (ISP)'s computer is a host. The number of hosts is an indicator for the Internet connectivity. As of July 2006, the number of Internet hosts reached 439 million (Internet System Consortium, ISC 2006). From the ISC (2006), the development of Internet hosts from 1969 to 2006 showed that the development was relatively slow in the first two and a half decades, and began to accelerate from the mid-1990s.

A significant aspect of cybersecurity is correlated with the accessibility to computers and networks. Occasionally, these computers and networks are the targets of cybercrime. In these cases, the damaged computers and networks become sources of losses suffered by users. As part of the hardware of the entire Internet, Internet hosts are also important reference factors when considering the prevention of cybercrimes.

The fourth indicator is the number of web pages. As of 2007, the Google search engine collected 8 billion of web sites, indexed nearly 10 billion of distinct web pages, several billion of all types of images: photos, drawings, paintings, sketches, cartoons, posters, and more. It is a complicated matter to correctly provide an accurate quantitative measurement of the growth rate of the Internet. The search engine and web site survey have been regarded as useful ways (Tehan 2002, p. 7). The increase of the number of web pages basically indicates that web-based information with positive value and with negative value is increasing simultaneously. The increase in web pages has had multiple influences on online users. The more the web pages are published, the easier the users can discover the appropriate contents, but the less successful the webmasters can maintain them. The faster the web pages are increasing, the more complicated the situation will be on the part of both webmasters and users in terms of obtaining information, maintaining the contents, and avoiding legal problems.

The fifth indicator is bandwidth growth. Bandwidth measures the capability of the communications channel. Bandwidth growth facilitates more users and more convenient online activities. The lowered cost and enhanced quality of services attract people of various ages, different income levels and educational background to join the online community. A longer online time also becomes possible. Therefore, bandwidth growth directly influences the number of online users, the length of online time, and the categories of online activities.

The sixth indicator is the growth of scale of e-commerce. UN (1997) noted that "an increasing number of transactions in international trade are carried out by means of electronic data interchanges and other means of communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communications and storage of information."[6] Although e-commerce is different from those above-mentioned factors that are directly related to the scale of the Internet, to some extent, nevertheless, we can quantify how many commercial opportunities and interests rely on cybersecurity. That is to say, any cybercrimes that shake the foundation of the Internet will have influences on e-commerce. Direct or indirect, tangible or intangible,[7] pecuniary or non-pecuniary losses can be caused by various kinds of cybercrimes. Therefore, a brief introduction to the growth of e-commerce is not meaningless. At least, in considering the cybersecurity investment and the cybersecurity financing, the scale of e-commerce can be a valuable parameter for making such estimate.

In fact, in the U. S. alone, five years after the introduction of the WWW, the size of Internet economy can compete with traditional sectors, such as energy, automobiles, and telecommunications (Centre for Research in Electronic Commerce 1999, p. 8). The Internet economy also rewrote the history of the employment market (Ibid, p. 9).

Integrity and reliability of information are important for e-commerce.[8] Along with the development of e-commerce, criminals are also transmitting their activities online. The increasing dependence of business on information and communications systems is gradually changing the global social-economic scenario.

In fact, besides e-commerce, many other industries more or less depend on information and communications systems. More people, more assets, and more activities continue to go online, the efficiency of social actions reaches an unparalleled degree on the one hand, the over-dependence on information and communications systems also brings about new risks that society would never have met without the systems on the other hand. It is unnecessary to overemphasize the catastrophic effect of the possible interruption of information and communications systems. However, we should bear in mind that the increasing dependence on information and communications systems would cause more and larger risks for the society. Social disorganization is usually associated with social change, particularly, innovation (Mowrer 1942, p. 32). The information society has the tendency of disorganizing in a more informed way.

The society is transiting from the process of urbanization to cyberization. An information supercontinent is taking shape. The increasing significance of the Internet for society and the accumulated threats of abuse deserve universal attention.

The following sections will analyse the fundamental properties of networked information and communications systems and their primary impacts on the maintenance of social order.

The uncontrollability of networked activities

ICT facilitates free and, frequently, a trans-territorial flow of information. The security of information and communications systems has also been a topic discussed in many literatures from very early years. For example, Bequai (1983, pp. 192-222), and Icove and co-workers (1995)

[6] UN General Assembly Resolution A/RES/51/162 (30 January 1997).

[7] Concerning costs of crime, see Levinson (2002), pp. 336-343, particularly, direct and indirect, tangible and intangible losses of general crime, see Levinson (2002), p. 338.

[8] This kind of recognition makes it imperative for international legal instruments to coordinate position of different countries, for example, Annex to UN General Assembly Resolution A/RES/51/162 (30 January 1997), the Model Law on Electronic Commerce of the United Nations on International Trade Law, Article 8.

covered a wide range of issues connected with computer security. It requires a special forum to provide an answer to the question of whether it is technically, morally, or legally suitable for the Internet to be managed, regulated, or controlled. But a fundamental conclusion is that the security of information and communications systems is only relative. Absolute cybersecurity did not in the past, does not in the present, and will not in the future, exist. Alexander Hellemans (1999) reported that, using a complicated algorithm and software, scientists broke the RSA-155 code, which is a popular means for protecting secret information on the Internet in Europe, even though it is an issue for researchers to spend 5 months on 300 PCs and a Cray 916 supercomputer (p. 1472).

This paper explores the difficulties in exercising control over the Internet. Controllability permits management to exercise a directing or restraining influence over its use, behaviour, and content (Fisher 1984, p. 24). Controllability of the Internet has a direct influence on cybersecurity. The concept of uncontrollability originates from the vulnerability of ICT acknowledged by the pre-Internet writers. Bequai (1978, pp. 9-17), for instance, divided the operation of the system into five stages (input, programming, Central Processing Unit, output and communication process) and asserted that each of these stages is vulnerable to attacks by the perpetrators. Bequai (1983, pp. 4-7) raised four reasons why computer technology is vulnerable: (1) it is vulnerable to abuse, particularly physical attacks and embezzlement; (2) it provides opportunities for various kinds of thefts; (3) it threatens every user with the development of human dependence on the machine; and (4) it functions in a “corrupt environment” where white-collar crime prevails. He concluded that “crimes by computer can be easy” (Bequai 1983, pp. 16-26).

Nevertheless, Kollock and Smith (1999, pp. 3-28) studied “the landscape of cyberspace”, and presented a constructive analysis of the social order in the Internet environment. This papper will emphasize and expand the analysis of the security problems usually involved in major Internet services. The characteristics of Internet services with special regard to controllability can be summarized in the following nine respects.

The universal accessibility of the Internet

Universal access to the networked information and communications systems can have both positive and negative roles in terms of social development and social control. Positive, because the society is networked and the networks are available to more and more members of society. Negative, because the traditional social networks have been replaced and the members are moving to and constructing new networks. The impotence of the old order and the absence of the new order will create an integration vacuum, to be expressed in the form of anarchy and chaos, for a process of disintegration and disorganization can be anticipated during this transformation (see Mowrer 1942; Elliot and Merrill 1961).

Since the removal in the 1990s of access constraints on the Internet for commercial use, the premises in which Internet access service is available have been rapidly extended. Besides regular users in schools and companies, cyber cafés and homes also facilitate the access of a significant number of users. In some countries, the management of cyber cafés forms the main path to cybersecurity. Cyber café has become the paradise of school-aged juveniles who play truant. Many problematic youths spend a long time in cyber cafés chatting, gaming, gambling, and entertaining. The cyber café is a place devoid of supervision and restraint as far as both private and public sectors are concerned. Neither families nor educational institutions can exercise control over activities in cyber cafés. In addition, the owners of cyber cafés are usually motivated by profits and do not care about the users' activities. For instance, many cyber cafés in cities and towns are opened unlicensed due to the failure to meet the requirements of the fire codes.[9] Besides the physical security and Internet addiction, the cyber cafés also involve cybersecurity concerns. Hackers and gangsters are increasingly crowding to the Internet, the cyber cafés being a paradise for them. According to the National Police Agency of Japan, more than half of computer crimes in 2005 were committed by using computer in cyber cafés. An increasing number of Japanese in their twenties and thirties, as well as many homeless people, select cyber cafés, which offer a "bed and Internet" package, as their home.[10]

It is not difficult to comprehend that some Asian countries have outlawed unlicensed cyber cafés. A measure of this kind matches crime prevention and crime control in other countries with a different political situation and cultural background. People from countries without the "cyber-café syndrome" definitely cannot approve such crime prevention measures, and usually protest against governmental actions that shut down cyber cafés. Such protests raise the issue of closing down these premises to the level of a human-rights question. It is then maintained that closure means a threat to information access and freedom of expression. Such a standpoint ignores security and crime concerns. Issues of rights and of crime are always interrelated. It is worth noting that in most European countries, thanks to better living standards, educational and other conditions for the development of a broad bandwidth, the cyber cafés are less developed. The full extent of the issue is thus neglected.

Universal accessibility does not mean that there are no different patterns of usage. People of different ages may spend a different length of time online in carrying out their different goals. People of different gender may exchange different information inside and outside their groups. People in countries in different developing stages may have a different Internet penetration ratio. People are all born equal, but equality of access to information has not been achieved, and equality does not mean sameness. Some people do not want any more information. The impact of information and communications systems on different individuals, groups, organizations and agencies is, therefore, one of different styles: beneficial or harmful, positive or negative.

The invisibility of cyberspace

Conventional countermeasures and theories about crime prevention were based on its material influence and on the material environment, although non-material factors have long existed, too. Activities in information and communications systems can be expressed in a physically invisible form. What are physically visible in information and communications systems are those physical existences, such as hosts and terminals, displayers, keyboards, mouse, and cables, while the mechanisms by which the computers function are invisible. Cyberspace is developed from information and communications systems as an abstract space, differing from the material devices

[9] Lu, L. Online Survivors in China, 13-20 April 2006, Beijing Review.

[10] Konstantin Kornakov, Cyber Café –or the Scene of Cybercrime, 5 March 2007. Retrieved 15 March 2016, from http://www.viruslist.com/en/news?id=208274049.

of information and communications systems that include terminals and cables.[11] It is invisible and intangible if compared with traditional space (Khosrow-Pour 1998, p. 440; Robertson 2000, p. 248; Dodge and Kitchin 2001, p. 81). When a web page is surfed, what can be seen is only the display of information on the screen. The web site is not physically a reading room where people can read magazines, newspapers and books, listen to audio records or watch videos, nor a marketplace, bank, street, or forum. It is merely a collection of web pages written in various mark-up languages, comprised of letters, numbers, and symbols in common use, but which facilitate the functions of linkage to other media, communicating with other people or directing to other services. The electronic address is not necessarily located along a street, in a building or even in a city, province, or country. In addition, the online services are usually provided in the manner of a remote transaction paid by means of digital cash or virtual money. Finally, the Internet users include individuals and institutions, but they do not necessarily appear in person or in an entity in a traditional library, forum, marketplace, bank, or along a street. It is entirely an invisible community in an invisible space.

The low controllability of the process

Since the early days of the computer and the Internet, efforts have not been lacking to control the system. Theoretically, the Internet can be controlled; however, actual and perfect control is unattainable. Thus, it is reasonable to say that the Internet can be controlled by any of the users if there is anyone trying to exercise control over part of it; but it cannot be controlled by any of the users if they want to exercise absolute control over the whole system. The low controllability by one means, on the other hand, the high possibility of control by many others. The low controllability by authorized users means the high possibility of control by unauthorized uses.

According to Kollock and Smith (1999, pp. 3-28), the Internet services have a very low controllability, even though it does not in my opinion greatly affect the social order. They explained the mechanisms of e-mail, Usenet, and WWW, which are the commonest means of communications and information exchange between online users. Both free and paid services are available online on an immense scale. E-mail lists, Usenet, and WWW are used to distribute messages simultaneously to all the subscribers of the lists or Usenet, or published for public access. To some extent, owners, administrators or servers of e-mail lists, Usenet and WWW have a certain degree of controllability when owners decide publish or refuse the messages. However, the openness of most e-mail lists, Usenet and even WWW enables users from everywhere to publish messages. To review a substantial quantity of messages requires considerable time and labour. What makes it a challenging social space is that any online users can write, publish, retrieve and save the contents, meaning that they expose themselves to anonymous users and trans-territorial users (see Kollock and Smith 1999, pp. 3-28).

Kehoe (1993) has discussed the situation of Usenet. He has claimed that the Usenet is not an organization, devoid of central authority; not a democracy, because democracy also requires organization; not fair, because unfair things will be discontinued by no one; nor a public utility, because of little or no control (pp. 36-38). Kingdon (1994) concluded that the Usenet control ends at the newsgroup level rather than at the individual level. Messages can be distributed among

[11] See description in Gibson (1984), etc.

thousands of computers worldwide, and the establishment of jurisdiction over disputes and offences is impossible.

Controllability of online instant messages is yet lower than the above-mentioned services. During the instant communication, the sending and receiving of the messages happen in a nearly synchronous manner. If these messages contain offensive contents, or hyper links to an offensive web page, there is no *sure* way of providing prearranged measures for precluding them. There do exist certain kinds of filtering and blocking mechanisms, but it is still a problematic matter whether these mechanisms are effective in passing and blocking the exact messages. While the filtering mechanisms are based upon logic coding under the hypothesis of rational human activity, the ways in which filtering and blocking programmes can be rendered invalid are simple and multiple. For example, the substitution of letters by similar numbers or symbols, or use of icons as words and phrases, is a method that is easy to use but difficult to filter.

Even if it is merely an individual e-mail, it is still confronted with uncontrollable threats. Kelly (2002) has mentioned the three primary aspects, that is, the loss of the confidentiality of e-mailed information, the distortablity and misinterpretation of content and the possible liability of an institution for the message as a publication.

The above analysis enables us to draw the natural conclusion that the control over the process of the Internet services is theoretically possible but practically unfeasible. The impossibility of control over the Internet immunizes individuals and institutions from any liability for the omission of such a control. Under these circumstances, neither an *ex ante* obligation nor an *ex post* liability can be adhered to as far as related individuals and institutions are concerned. Thus the incentive for control will hardly be strong.

The disputability of content and activities

The old and new diversity between cultures, societies and laws has not necessarily been diminished by the common networks of information and communications systems. On the contrary, universal information and communications systems bring in a diversity from offline to online, and bring about a diversity between offline and online. For example, we see that while there are different versions of religious classics on the networks, there are also different versions of political works online. People have the equivalent chance to read various versions of holy books. If they are to establish a belief different from their previous ones, they are equally likely to be influenced by this version or that version. Thus, from the viewpoint that information and communications systems form a space accommodating different cultures and ethnicities, we cannot expect too much of them, because they have the power both to create and to some extent eliminate diversities. The connection of the Internet to current legal frameworks, including restrictions on displaying unfeasible materials, the protection of privacy, and the limits of permitted business all become the subject-matter of major legal argument.[12] This has become a well-established conclusion.

The capacity of an uncomplicated publishing process makes the web pages an important media for businesses and individuals wishing to convey information to almost as many people as possible (Williams 2001). Every online user is able to contribute to certain kinds of publications: scholars shift their academic journals to inexpensive and easy-spreading digital versions; students

[12] Citron and Toronto Mayor's Committee v. Zundel, 2002 CanLII 23557 (C.H.R.T.).

put their essays on the bulletin-board system; and dissidents establish web sites to publish statements against the political authorities. In addition to technological problems, online content also involve two aspects of legal problems: the protection of free speech in some countries and the prohibition of offensive speech in some other countries. Freedom of speech or freedom of opinion and expression is provided as basic human rights in international agreements and domestic constitutions.[13] Many countries have similar clauses in their constitutions. Although the literal wording in the constitutions may be similar, the judgment standards of free speech are different. What is visible is only the wording of the clauses, but what is invisible is their legal spirit. In some countries, the law of free speech protects online messages, and refusal of publication requests and deletion of published messages may bring about legal disputes. In some other countries, these messages may be legally or religiously offensive. Even within one country, there is also the possibility that the courts rest on positions different from each other or different from the relevant legislation. For example, in Reno v. American Civil Liberties Union,[14] the court struck down a federal provision prohibiting the ending or displaying of obviously disgusting material in a style available to anyone less than eighteen years of age. The court ruled that the prohibition violated the First Amendment.[15] In Ashcroft v. Free Speech Coalition et al.,[16] the Supreme Court of the U. S. upheld the Child Pornography Prevention Act of 1996 (CPPA), which expands the federal prohibition on child pornography to both pornographic images made using actual children and “virtual child pornography.”

These factors determine that controllability of the Internet, the legal foundation of control, the willingness to control, and actual control over the Internet are conditionally dependent. Under such circumstances, it is not groundless for technological supremacists to suppose that the Internet lists will assist in the realization of their anarchist ideal.

For example, with the help of the Internet, the pornographic economy has developed on a great scale. It is true that obscene texts, graphics, and audio and video files have a different status in different cultural contexts. They may be legal for all people. They may also be illegal for all people. However, in most cases, they are legal for adults, but illegal for juveniles. In addition, the content of obscene files does not matter: description or illustration of children often render the whole file illegal, because this is regarded as sexually exploiting children. In any case, if the file is illegal, acts with the intent to create, record, possess, present, publish, replicate, disseminate, trade, advertise and so forth are all illegal. Even collecting and enjoying them by oneself will be

[13] In The Universal Declaration of Human Rights 1948, Article 19 prescribed that “Everyone has the right of freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive, and impart information and ideas through any media and regulations of frontiers.”

Other primary international agreements including freedom of opinion and expression are The International Covenant on Civil and Political Rights, Articles 19 and 20; The International Convention on the Elimination of All Forms of Racial Discrimination, Articles 4 and 5; The American Convention on Human Rights, Article 13; The African Charter on Human and People’s Rights, Article 9; The European Convention on Human Rights, Article 10; The European Convention on Human Rights, Article 10, etc. For more information, see Lawson (ed. 1996).

[14] Reno v. American Civil Liberties Union (Supreme Court No. 96-511, 26 June 1997).

[15] Fallon (2004), p. 53. The First Amendment was implemented in 1791 prescribed that “Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.”

[16] Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002), Docket No. 00-795 - April 16 2002.

punished. According to the Penal Law of Finland, dissemination of the depiction of obscenity, possession of obscene pictures of children and unlawful marketing of obscene material are all criminalized.[17] However, that the incentive of benefiting from the commercial transaction of pornography motivates the Internet content providers or Internet users means that it is difficult to control the Internet content.

In addition to the fact that the digital form of traditional verbal, written, printed, audio as well as video content inherits these above-mentioned traditional prohibitions, the Internet further inherits the problem enforcing the illegal nature of some activities, such as gambling, along with the trade in some materials, such as drugs, philtres, and weapons. Some of these fields are in dispute. The most controversial issue may be the criminalizing or legalizing of gambling and marijuana. The momentousness of these topics in contemporary society has attracted the attention of multitudinous studies and research. Now, despite their legal status in different countries, exchange of information about these activities and materials, transaction and payment, necessary offline delivery of goods, and possible internationally prohibited money transfer in some areas, may create unsolvable problems for control over the Internet.

Information and communications systems can accommodate contents of different value-orientation and activities of a differing legal nature, usually creating controversies among the various jurisdictions. As a result, the authorities in the country where the content or activities are legal cannot provide sufficient protection for people who publicize legitimate speech or carry out legitimate activities, and cannot prohibit infringements and impose sanctions on people who infringe these legal rights. Similarly, authorities in a country where the contents or activities are illegal cannot impose sanctions on people who breach the proscription, and cannot protect people who obstruct the illegal contents or activities from wrong prosecution by a country where people adopt contrary standpoints to the legal nature of these contents or activities. In Europe, this dispute exists in the respect of speech concerning the identification of several historical incidents, such as the genocide of certain races, denial of which may induce criminal prosecution in countries including Austria, Belgium, the Czech Republic, France, Germany, Italy, Lithuania, the Netherlands, Poland, Romania, Slovakia, and Switzerland. Denial of the historical occurrence of genocide is also punishable in Israel.[18] In spite of some international conventions, the problems of this paragraph are not in practice more easily dealt with than the problems of the proceeding paragraph.

The divisibility of digital files

Division is a threat to most forms of life and most forms of existence. However, at the same time, division means life and the existence of digitalized information. Digital files exist in information and communications systems and are transmitted through the networks in particular forms. Erol (1992) described it as a process of "moving bits from one place to another" (p. 19). In transmitting processes, a file is regularly broken into many packets conveyed along the networks in different jurisdictions. For example, if a European user sends a message from his or her room to the

[17] Penal Code of Finland, Chapter 17, Sections 18-20 (563/1998).

[18] Wikipedia, Holocaust Denial. Retrieved 15 March 2016, from http://www.wikipedia.org/wiki/Holocaust_denial

neighbouring room, the message may be divided into several packets. When they are transmitted from one room to another through the Internet, there is the possibility that all packets are transmitted directly through local networks and arrive at the destination. Nevertheless, there exists, too, the possibility that certain packets transmitted to North America, and then to Africa, or Asia at last arrive in the neighbouring room. It is a frequent phenomenon for a single e-mail message to traverse countries in different continents. If every country attempts to exercise jurisdiction, the process can become exceedingly complex and unmanageable. Plainly put, it may occur that one particular country may simply be crossed by certain packets.

Most of the Internet services involve some kinds of file transmission. For example, contents of e-mail, Usenet, chat room, and web page are generally transmitted as files and divided into packets during the process. Different packets may be transmitted via different routes and different jurisdictions. Even though in reality information is not divided as extremely as we imagine, the possible gap and overlap of legislations have still become a major problem.

The low confidentiality of information and communications systems

Protected data in information and communications systems should be "obtained and processed fairly and lawfully."[19] Technical and organizational measures should be taken to protect personal data against access without authorization, manipulation, disclosure, transfer and other processing without legal reason.[20] Besides general protection of personal data, sensitive personal data are granted special protection by law.[21] Exceptions are derogations,[22] which are prohibited to process.[23]

Information and communications systems are usually analogous to a place with unrestricted freedom and where the information is less confidential. Weak technical control and weak human control are the main factors that expose the weakness of the systems. The most obvious example is e-mail. The technical mechanisms demonstrate that e-mail has exceptionally low confidentiality, and is more vulnerable to disclosure than traditional letters. Without encryption, every document sent by e-mail is publicly accessible, and system administrators can easily view every outgoing and incoming e-mail without any preceding authorization (Sikorski and Peters 1999, p. 348). Kelly (2002) mentioned that the confidentiality of e-mailed information can be lost in such cases as when it is intercepted, when it is sent to a wrong address, or when it is read by an unauthorized or unintended person.

In addition to less prepared gaze, Rogers (2001) worried that the governmental agencies, business organizations and other individuals are usually motivated to abuse their powers and rights

[19] Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 5; Directive 95/46/EC, Article 1 (a).

[20] Convention Article 7; Finnish Personal Data Act 523/1999, Section 32 (1).

[21] According to Finnish Personal Data Act 523/1999, Section 11, sensitive data include data relating to or are intended to relate to the following aspects: "(1) race or ethnic origin; (2) the social, political or religious affiliation or trade-union membership of a person; (3) a criminal act, punishment or other criminal sanction; (4) the state of health, illness or handicap of a person or the treatment or other comparable measures directed at the person; (5) the sexual preferences or sex life of a person, or (6) the social welfare needs of a person or the benefits, support or other social welfare assistance received by the person."

[22] Finnish Personal Data Act, Section 12.

[23] ibid, Section 11.

to infringe e-mail privacy. The secrecy of individual interaction in sending and receiving e-mails online is easily destroyed, because of being unencrypted. It is possible for hackers to tamper with the e-mail, or for the Internet service providers (ISPs) to check the packets, resulting in loss of users' e-mails and disclosure of individual privacy or business secrets. This is no different from clandestinely opening other people's letters, encroaching upon other people's correspondence secret (Wang 2001, p. 154).

Computer processing enables "interceptions to be multiplied a hundredfold and to be analysed in shorter and shorter time spans."[24] The interception of electronic correspondence has been legalized under different conditions in many countries. For example, according to the U. S. Electronic Communication Privacy Act (ECPA),[25] ISP may supervise or intercept e-mail information for normal commercial goals and in order to protect property or related right. In addition, in the workplace, it is deemed that the employees have no privacy in company computers.[26] Apart from legally authorized interception, infringement of privacy also poses a great concern.

In fact, many court decisions in the U. S. have rejected the expectation of workplace privacy. At workplace, employers and governments provide information and communications systems for work-related use only. Law and policy limit any use for non-work functions. The logic is that the use of information and communications systems for non-work purposes is a breach of law and policy and deemed misconduct; then, the search into the personal use of these systems does not breach the privacy rights of their employees.[27]

The mobile networks are as vulnerable as the traditional computer networks. Security loopholes usually threaten individual rights and state security. According to the Finnish government news, a serious data security problem has been discovered in the Finnish Ministry of the Interior. With this kind of problem, it became possible to listen to the mobile phone calls of thousands of employees without authorization. Consequently, the Ministry had to inform the employees not to use mobile phones for confidential aims. The problem concerns employees in the police and rescue forces, emergency services, the Border Guard, the Directorate of Immigration, the Population Register Centre, and employees within the Ministry of the Interior itself.[28]

Anonymity

[24] Malone v. The United Kingdom - 8691/79 [1984] ECHR 10 (2 August 1984).

[25] 18 U.S.C. §§ 2510-2522; and 18 U.S.C. §§ 2701-2711. The Act amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (the Wire Tap Statute).

[26] For example, in United States v. Ziegler (No. 05-30177 D. C. No. CR-03-00008-RFC ORDER AND OPINION, 6 March 2007), the government argued that:

"Society could not deem objectively reasonable that privacy interest where an employee uses a computer paid for by the company; Internet access paid for by the company, in the company office where the company pays the rent…This is certainly even more so true where the company has installed a firewall and a whole department of people whose job it was to monitor their employees' Internet activity." (p. 1087)

[27] See United States v. Wesley George Thorn, No. 03-3615, Federal Circuits, Eighth Circuit (July 13, 2004); United States v. Angevine, 281 F.3d 1130, 1134–35 (10th Cir.); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000), etc.

[28] Finland Government News, Data Security problems in Ministry Mobile Phones, 15 February 2006. Retrieved 15 March 2016, from http://e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=47840

The disappearance of physicality in activities on the Internet symbolizes the new way for daily routines, and presents a chance for new practice and changes in faiths, positions, and manners (Zigrus 2001, p. 171). To a certain extent, Internet services are provided for every user who owns a computer and a modem or cable linked to the server. The real identity of the user is not necessary for using the Internet. That is to say, a high degree of anonymity is achievable. Anonymity could indicate an intention to lie or not, to do something deceit or not. In the environment of online communications, particularly during interaction between remote strangers, information and communications systems provide the possibility of maintaining anonymity, and we found that the users of information and communications systems have the willingness to stay passively anonymous, not necessarily actively lying to their counterparts.

In the case of e-mail, it is uncomplicated to register an e-mail account with false information, or to send messages in the name of a certain person. These e-mails may not only infringe the legal rights and interests of the person of the counterfeited identity, but also are able to fabricate a rumour, slander other people, harm other people’s reputation, or practise unfair competition to reduce the competitor’s trustworthiness. No obligation of free e-mail service providers has been established to investigate the registrants’ identity information. In addition, some web sites also provide anonymous e-mail services or sell anonymous e-mail software.[29] Under such circumstances, the traceback of the real sender is impossible. Only where the providers’ status is clear, under vicarious liability, can it be useful for law enforcement in some jurisdictions to hold the re-publisher responsible for the content of the original author (Edwards and Walde, eds. 1997, Part 4).

E-mail has frequently been abused in an anonymous way so as to realize a fraudulent scheme. This anonymity not only facilitates a lie, but may also support a fraud. In R. v. Mastronardi,[30] the accused, met the plaintiffs through an Internet dating service, during which the accused misrepresented himself as a single person and engaged in relationship with several victims. He represented himself as:

“(a) coming from a large, powerful and wealthy Sicilian family;

(b) being a widower seeking a wife;

(c) being a medical doctor with a specialty in gynaecology;

(d) having hospital privileges and a clinic;

(e) being a kind, caring and considerate person with positive family and moral beliefs, conveyed in conversations that went on for hours on end;

(f) having elaborate and sometimes bizarre family and cultural traditions requiring highly submissive wives and amalgamation of finances to an account controlled by him;

(g) as time went on, being third in command in mafia like family organization;

(h) not wanting to date, but wanting to immediately enter into an intimate relationship, after which his culture and family regarded them as married;

(i) once so married, his family required him to follow family and cultural traditions.” (paragraph 4)

In R. v. Farkas, the accused engaged in online fraud by using different e-mail addresses, mailing addresses, and user names, victimizing sellers and purchasers distributed in the U. S.,

[29] Examples of such services and software can be searched out with search engines.

[30] 2006 BCSC 1681.

Canada, and England.[31] In R. v. Reynolds & Ors, the accused engaged in online chat claiming himself to be a 16-year-old boy, attempting to make young girls expose their bodies and transmit photographs to him over the Internet.[32]

There are many ways by which people make efforts to detect lies, usually including various clues to emotion that may disclose the situation of lying (Ekman 1992, as cited in Howitt 2002, pp. 251-253). However, in the electronic lie, none of the clues can be useful, particularly those emotional ones, because there is no face-to-face interaction. Rather, the interaction itself is covered by a human-machine-human fig leaf.

Another field where people usually maintain anonymity is interaction in chat rooms. Accounting for a considerable fraction of the income of the commercial online providers, chat systems support synchronous communication, discussion on different topics, trans-territorial relationships on common interests, and ignorance of social status (Internet Crime Forum IRC subgroup 2001, pp. 7-9; Rowland 1998; Wilbur 1997, p. 5.). The biggest advantage of the interaction in chat rooms is that the user can keep anonymous at the beginning of the chat or remain anonymous during the whole process. Keeping anonymous means that people are able to fabricate identities that cannot be used to identify them. By disguising themselves, users can perpetrate fraud and many other related activities. This approach is definitely useful, too, in detection and investigation of crimes, where law enforcement uses falsified identity to allure and arrest suspects.[33] The actual reality is that, in information and communications systems, determining users' identity proves difficult, but not impossible.[34]

The abuse of services

The powerfulness of the Internet facilitates instant communication and timely information exchange, covering an unlimited range of messages and information, desirable or undesirable, legal or illegal, beneficial or anti-social. The convenience of e-mail for communications is frequently exploited as the fastest and easiest ways of spreading computer viruses, spam, and frauds over the Internet.

The e-mail is the primary means for spreading malicious programmes. For example, the Love Bug virus reached millions of computers within 36 hours of its release from the Philippines thanks

[31] 2006 ONCJ 121, 10 April 2006.

[32] [2007] EWCA Crim 538 (08 March 2007).

[33] For example, in United States v. Helder (Eighth Circuit, No. 05-3387, 16 March 2006), an undercover officer used a screen name and claimed to be a 14-year-old girl to entrap the perpetrator (pp. 2-4); in United States v. Baker (Seventh Circuit, No. 05-2499, 24 January 2006), an undercover officer used a screen name and claimed to be a 14-year-old boy to entrap the perpetrator (pp. 2-3); in United States v. Antelope (Ninth Circuit No. 03-30557, 8 June, 2004. Docket num. 03-30334, January 2005), the accused joined an Internet site advertising "Preteen Nude Sex Pics" and started corresponding with an undercover law-enforcement agent, in respect of whom the accused was entrapped when he ordered a child pornography video over the Internet; in United States v. McGraw (Tenth Circuit No. 02-1407, D. C. No. 01-CR-426-B, 2 December 2003), the accused was also caught by an undercover agent, with whom he expressed his interests in "having sexual contact with 'white males between the ages of 12 and 15'," and arranged a encounter. See also R. v. Randall (Provincial Court of Nova Scotia 2006 NSPC 19, No. 1538177, 28 April 2006).

[34] As Peter Steiner's cartoon saying that "On the Internet, Nobody knows you're a dog." Originally appeared in The New Yorker, volume LXIX, number 20, 5 July 1993, p. 61. Retrieved 15 March 2016, from http://www.unc.edu/depts/jomc/academics/dri/idog.html

to e-mail. Subsequently, these malicious programmes can send messages, collect information, delete data, spread a Trojan horse, or plan future accidents (Sadowsky and co-workers 2003, p. 48). At the same time, e-mail bombing, that is, sending a large amount of e-mails to the victim, can crash the victim's e-mail account or servers (Syngress 2002, p. 325). Therefore, a security concern is closely related to e-mails.

The e-mail is both the means and the target of spam, utilized primarily for commercial, political, malicious, or illegal schemes. As a marketing and communications means, e-mail has been gradually abused. Recipients of unsolicited e-mails have to spend much time to deal with messages, wasting human resources and baffling the receiving of useful messages. The sending of bulk mails also consumes network bandwidth and interferes with the ordinary communications service. In addition, unsolicited commercial mails are usually sent anonymously or with a fabricated identity, and the recipients cannot stop subsequent messages. Messages of this kind also include false or misleading headers, deceiving recipients to retrieve messages that they do not want. Moreover, the recipients have no way of expressing their wish not to receive such messages, and have no way of requesting compensation even if they suffer loss. The abuse of e-mail has become a public nuisance in the online environment. Although the use of anti-spam services and technologies is increasing, the scale of spam is continuing to increase as fast (OECD 2004, pp. 2-3; OECD 2005, p. 6), becoming a problem not only for personal e-mail accounts, but also for corporate accounts. In regulating the legal problems which the e-mail brings, traditional criminal law has insufficient coverage.

Cyberstalkers also abuse the e-mail service by sending text-, graphic-, and audio-based messages of a threatening, alarming, or harassing kind to the e-mail account of the intended victim (D'Ovidio and Doyle 2003, pp. 10-17). At present, it is also possible for a video-based message to accomplish the equivalent effect. Other Internet services can also be exploited by cyberstalkers to harass other users, either directly or indirectly. An example of direct harassment can be found when stalker sends harassing messages to a targeted victim. An example of indirect harassment can be found when a stalker uses the Internet communications to obtain a potential victim's personal information, such as a home address etc., and then uses the information to contact by other means. In these cases, children are frequent victims (Internet Crime Forum IRC subgroup 2001, p. 11).

In many incidents, what has been revealed is "the all too common failure of both public and private sector organizations to ensure that safeguards are identified and diligently implemented throughout organizations."[35] Due to the abuse of online services, it can be said that, on the Internet, the use and abuse of the services grow hand-in-hand; and chances and challenges exist simultaneously.

From information society to mobile society: the uncertainty of the future

In the technological field, what is certain is the tendency of ceaseless advancement, but what is uncertain is the outcome of this ceaseless advancement. ICT is the most dynamic field in the present world. Network technology is one of its relevant aspects. In addition to the traditional

[35] Sale of Provincial Government Computer Tapes Containing Personal Information, Re, 2006 CanLII 13536 (BC I.P.C.).

networks, mobile and wireless networks have been developing rapidly in recent years. The goal of the new network technology is to integrate the known advantages of the previous network, avoiding the known disadvantages, while creating the unknown advantages. The most advantageous characteristic of all the networks is the decentralized structure, without central control. The unique advantage of mobile phone and wireless networks is the possibility of wider spatial separation between terminals and network devices. Controllability of such networks is being transformed into new forms. At the same time, the existing security concern has also been transplanted into the new media (Karygiannis and Owens 2002, pp. 21-22). The future of technology and security are unforeseeable.

Computer networks form an uncertain phenomenon with which the legal system should keep pace. In the last few years, people in the U. K. were fond of quoting an estimate according to which the U. K.'s currency reserves can be transferred outside the country in fifteen minutes Kelly 2002). Both the convenience and dangerous nature of information and communications systems are imaginable. With the traditional network, the online threats emerged about when the wire, fibre and cable of the network were to be linked. At the moment, with wireless and mobile networks, the invisible threats are emerging in space where the electromagnetic wave of the network covers. Although the new technological outcomes are always accompanied by corresponding safeguards, historical instances have proved that the initial measures have usually been less effective. In addition, the legal framework is less ready and less prompt in reaction to the new phenomenon. As Clarke claimed that, with cybercrime (computer viruses), the collapse of banks, the launching of nuclear missiles, the shutdown of air traffic control, and the paralysis of the telephone network are all possible in the future (Clarke 1997, p. 227).

Conclusion

The Internet creates a space without a spatial or temporal boundary. Anyone with Internet access is connected to everyone else with Internet access in the world and is likely to be affected by the information that is published and the activities that are facilitated. All that not only provides chances for a social life, but also poses challenges to the social order. As a result, Gates (1995) stated that a significant aspect of the Internet is to get rid of remoteness, making it no difference between contacting a person in the next room and contacting another on another continent.

On the other hand, security and trust become essential to this new environment, which is constructed on systems vulnerable to attacks or abuse. Computers play different roles, such as means, media, target, tool, place, route in offences, and can be used in varied ways to prepare for other offences. People have already recognized that the unique character and the great value of the Internet for the user community is its decentralized structure (Rotenberg 1990, p. 16). What is tricky is that the maintenance of cyberspace order proves a challenge to the legal system. Many people are aware of the risks that people take when they go online. Quirchmayr (1997) pessimistically declared that the Internet became a paradise for all sorts of criminals (cited in Siponen 2001, p. 24). Interpol (2003) summarized the major threats as unauthorized access to and destruction of information in the processing, transporting, and storing stages. Information and communications technology poses enormous challenges to society, and clearly requires criminal-law reform.

Firstly, the objects requiring the protection of the criminal law have been expanded in the information age. The basic logic behind this is that, person, property and information are the three kinds of objects to be protected by criminal law, and that while both infringements of person and property are punishable offences, so should the abuse of information and communications systems punishable, too. Although criminal law has protected copyright, patent, trademark, and trade secret, the explicit literal provision for protecting "information" in criminal law is a development of the three recent decades. However, the provisions of different countries are not uniform. Disputes over changing the traditional criminal law are still taking place in some countries, and show the persistent resistance of the conventional notion. All these factors render the renovation of legislation an inefficient process. In order for criminal law to have actual effect, the sooner the renovation of the general theory and general part of criminal law are carried out, the better the criminal law can serve the information society.

Secondly, because of the expansion of the objects to be protected in the criminal law, it is very important to provide definition of new types of crimes, and to revise constituent elements of old crimes, in which information and communications systems become a new tool, object, place, medium, route, and means of traditional offences. This situation calls for the change of the special part of criminal law. If we say that the lag in the general theory of criminal law wastes resources in the legislation, the failure of the special part of the criminal law waste the resources in criminal justice, leaving a blank in deterrence as far as new types of crimes and new forms of old crimes are concerned. The effective implementation of domestic criminal laws increasingly depends on international coordination and cooperation, requiring realization to a far greater degree of the international consensus of substantial and procedural law.

Thirdly, the space of criminal justice is expanding beyond traditional society. The traditional crimes are fundamentally intra-national, trans-national, or at most international, while the new-fashioned cybercrimes are easily super-national and even virtual. That is to say, the crimes surpass the national power, while the super-national power in criminal justice has yet to be formed, being , restricted by the traditional principles of jurisdiction. In order to fill up the gap between the crimes and the power of criminal justice, international criminal law has formulated some new rules, though they are not widely accepted. A wider range of international action should be adopted in order to reduce the large expenses of time, money and human resources, and to decrease the further losses caused by crimes that are left unpunished in the process when there is this gap in criminal justice.

Fourthly, balance has not been reached between the influence of technology on criminal justice and on criminal phenomena, both of which are complex and involve positive and negative forces. The negative effect of technology on criminal justice and the positive effect on criminal phenomena point to a further failure of traditional criminal law: the inability of criminal justice and the inefficient deterrence against cybercrime increase the expected criminal benefits and lower the expected punishment. As a result, the increase of cybercrimes is inevitable. To resolve this problem, prompt enactment of domestic legislation worldwide and negotiation for international cooperation are required.

Fifthly, the dependence of criminal law on technology, and the interaction and mutual support between criminal law and technology should reach an unprecedented extent. Without the interaction of technology, criminal law could not obtain so great a deterrent effect. Similarly, without criminal law, technology could hardly function solely in crime prevention. Both of them are necessary, but not sufficient. Although adding them up is not sufficient either, integrated countermeasures are of the utmost importance in cybercrime prevention.

In sum, the weak controllability of the Internet poses serious problems that fall into the domain of criminal law. There is a necessity for translating traditional law to cyberspace, translating domestic law in the international forum, and translating diversified provisions into a unified standard. Criminal-law reform is to put an end to the disorder of cyberspace where obligations and liabilities have not been sufficiently established and perpetrators of offences often run large.

However, we should also notice that the information society is not a new society but a new stage of the existing society, a social reality that is being re-expressed in the form of a re-encoding with a new coding system, as well as a new social order that is re-coping with the developmental tendency of society that has emerged in this new form. In the re-encoding process, the old codes remain or disappear, while the new codes emerge and grow. Cybercrime is one code in the re-encoding process of the information society.

REFERENCES

1. Bequai, A. 1978. *Computer Crime*, Lexington, Massachusetts, Toronto: Lexington Books.
2. Bequai, A. 1983. *How to Prevent Computer Crime: A Guide for Managers*. New York, Chicago, Brisbane, Toronto, Singapore: John Wiley and Sons.
3. Centre for Research in Electronic Commerce. 1999. *Measuring the Internet Economy*, The University of Texas at Austin.
4. Clarke, A. C. 1997. *3001: The Final Odyssey*, Hammersmith, London: Voyager.
5. Dodge, M. and Kitchin, R. 2001. *Mapping Cyberspace*, New York, New York: Routledge.
6. D'Ovidio, R., and Doyle, J. 2003. A Study on Cyberstalking: Understanding Investigative Hurdles, *The FBI Law Enforcement Bulletin*, volume 72, pp. 10-17.
7. Edwards, L. and Walde, C. (eds.). 1997. *Law and the Internet - Regulating Cyberspace*, Oxford: Hart Publishing.
8. Ekman, P. 1992. *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*, New York: Norton.
9. Elliot, M. A. and Merrill, F. E. 1961. *Social Disorganization*, fourth edition, New York, Evanston, and London: Happer and Row Publishers.
10. Fisher, R. P. 1984. *Information System Security*, Prentice-Hall.
11. Forcier, R. D. and Descy, D. E. 2002. *The Computer as an Educational Tool*, third edition, Englewood Cliffs, New Jersey: Merrill-Prentice Hall.
12. Gates, B. 1995. *The Road Ahead*, New York: Viking.
13. GeoHive. 2006. Countries with Most Personal Computers. Retrieved 15 March 2016, from http://www.geohive.com/charts/charts.php?xml=ec_inet&xsl=ec_inet_top2
14. Gibson, W. 1984. *Neuromancer*, New York: Ace Books.
15. Grabosky, P. 2000. Cyber Crime and Information Warfare, The Transnational Crime Conference convened by the Australian Institute of Criminology in association with the Australian Federal Police and Australian Customs Service and held in Canberra, 9-10 March.

Retrieved 15 March 2016, from http://www.aic.gov.au/conferences/transnational/grabosky.pdf

16. Helmkamp, J., Ball, R., and Townsend, K. 1996. Proceedings of the Academic Workshop: “Definitional Dilemma: Can and Should There Be a Universal Definition of White-collar crime?” Morgantown, West Virginia: National White-collar crime Centre.
17. Howitt, D. 2002. *Forensic and Criminal Psychology*, Essex, England: Pearson.
18. Icove, D., and co-workers. 1995. *Computer Crime: A Crimefighter's Handbook*, O'Reilly and Associates.
19. Internet Crime Forum IRC Subgroup. 2001. *Chat Wise, Street Wise-Children and Internet Chat Services*.
20. Internet System Consortium (ISC). 2006. Internet Domain Survey. Retrieved 15 March 2016, from http://www.isc.org/index.pl?/ops/ds
21. Internetworldstats.com. 2007. Internet Usage Statistics-The Big Picture. Retrieved 27 July 2007, from http://www.internetworldstats.com/stats.htm.
22. Internetworldstats.com. 2015. Internet Usage Statistics-The Big Picture. Retrieved 15 February 2016, from http://www.internetworldstats.com/stats.htm.
23. Interpol. 2003. *IT security and Crime Prevention Methods: Explanations: A Report*. Retrieved 15 March 2016, from http://www.interpol.int/Public/TechnologyCrime/CrimePrev/ITSecurity.asp
24. Karygiannis, T., and Owens, L. 2002. *Wirelsss Network Security, 802.11, Bluetooth and Handheld Devices*, NIST Special Publication 800-48.
25. Kehoe, B. P. 1993. *Zen and the Art of the Internet*, Englewood Cliffs, New Jersey: PTR Prentice Hall.
26. Kelly, J. X. 2002. Cybercrime - High Tech Crime, JISC Legal Information Service - University of Strathclyde. Retrieved 15 March 2016, from http://www.jisc.ac.uk/legal/index.cfm?name=lis_cybercrime
27. Khosrow-Pour, M. 1998. *Effective Utilization and Management of Emerging Information Technologies*, Hershey: Idea Group Publishing.
28. Kingdon, J. 1994. Shooting the Messenger: The Liability of Internet Service Providers for Prohibited Expression. Retrieved 15 March 2016, from http://www.catalaw.com/logic/docs/jk-isps.htm
29. Kollock, P. and Smith, M. 1999. Communities in Cyberspace, in: M. Smith and P. Kollock (eds), *Communities in Cyberspace*, London: Routledge, pp. 3-28.
30. Levinson, D. (ed.). 2002. *Encyclopedia of Crime and Punishment*, Newbury Park, CA: Sage Publications.
31. Li, X. (2008). Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society. (Univerrsity of Turku). Turku, Finland: University of Turku.
32. Mowrer, E. R. 1942. *Disorganization: Personal and Social*, Chicago, Philadelphia, New York: J. B. Lippinatt Company.
33. OECD. 2004. *Second Organization for Economic Cooperation and Development Workshop on Spam: Report of the Workshop,* JT00174847, Busan, Korea, 8-9 September.
34. OECD. 2005. Task Force on Spam, Spam Issues in Developing Countries, DSTI/CP/ICCP/SPAM(2005)6/FINAL, Paris, France, 26 May 2005.

35. Pew Research Center. (2015). Social Networking Fact Sheet. Retrieved 15 February 2016, from http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/
36. Quirchmayr, G. 1997. Selected Legal Issues Related to Internet User, *The Third International Conference on Reliability, Quality and Safety of Software Intensive System*, Athens, 29-30 May.
37. Robertson, S. 2000. The Digital City's Public Library: Support for Community Building and Knowledge Sharing, in Ishida, Toru and Isbister, Katherine eds. *Digital Cities: technologies, Experiences, and Future Perspectives*, Springer, pp. 246-260.
38. Rogers, L. R. 2001. *E-mail: A Postcard Written in Pencil*, Pittsburgh, PA: Carnegie Mellon University. Retrieved 15 March 2016, from http://www.cert.org/homeusers/email_postcard.html
39. Rotenberg, M. 1990. Prepared Testimony and Statement for the Record on Computer Virus Legislation, *Computer and Society*, volume 20, number 1, pp. 12-25.
40. Rowland, D. 1998. Cyberspace - A Contemporary Utopia? *The Journal of Information, Law and Technology*, volume 1998, number 3. Retrieved 15 March 2016, from http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1998_3/rowland/
41. Sadowsky, G., Dempsey, J. X., Greenberg, A., Mack, B.J., and Schwartz, A. 2003. *Information Technology Security Handbook*, Washington, DC: The International Bank for Reconstruction and Development.
42. Sikorski, R., and Peters, R. 1999. NET TIP: Digital Security, Part I, Science, 15 January, vol. 283. no. 5400, pp. 348 - 349, DOI: 10.1126/science.283.5400.348b.
43. Siponen, M. T. Five Dimensions of Information Security Awareness, *Computers and Society*, June 2001, pp. 24-29.
44. Summers, D. (director). 2003. *Longman Dictionary of Contemporary English*, Essex, England: Pearson Education Limited.
45. Syngress. 2002. *Scene of the Cybercrime: Computer Forensics Handbook*, Rockland, MA: Syngress Publishing.
46. Tehan, R. 6 February 2002. CRS Report for Congress, *Internet Statistics: Explanation and Sources*, Order Code RL31270.
47. UN. 2000. Crimes Related to Computer Networks: Background Paper for *the Workshop on Crimes Related to the Computer network, Tenth UN Congress on the Prevention of Crime and the Treatment of Offenders*, Vienna, 10-17 April. A/CONF. 187/10.
48. Wang, Y. 2001. *Hulian Fawang: Zhongguo Wangluo Falv Wenti* (Interlink Legal Web: Problem of Chinese Cyberlaw), Economic Management Press.
49. Wilbur. S. 1997. An Archaeology of Cyberspace: Virtuality, Community, Identity, in D. Porter, (ed.), *Internet Culture*, London: Routledge, pp. 5-22.
50. Zigrus, I. 2001. Our Virtual World: The Transformation of Work, Play, and Life via Technology, IGI Global, 2001.