Crucial Elements in Law Enforcement against Cybercrime

Xingan Li*

* International Institute for Innovation Society, Helsinki, Finland

e-mail: xingan.li@yahoo.com

ORCID ID: 0000-0001-5409-8988

Research Paper Received: 19.04.2018 Revised: 10.09.2018 Accepted: 16.09.2018

Abstract- Technological innovation, globalization, and urbanization have facilitated criminals and terrorists to pose a fresh wave of hazards that can shake the security establishment of global markets. The development of information and communications technology creates not only advantages, convenience and efficiency, but also disadvantages, challenges and threats. The purpose of this paper is to explore into crucial elements in combating cybercrime. The paper identified the following crucial elements as special perpetrator-victim relationship, time elements, spatial elements and technological nature of cybercrime, complexity, costs, anonymity, hidden victims, concealment, trans-territoriality, and fast increase in recent four decades. They should be emphasized in fighting against cybercrime. The paper further analyzes the phenomenon of rent-seeking from the exaggeration of insecurity and cybercrime, which can be misinformation in this battle.

Keywords- Cybercrime; Crucial elements; Victimization; Motivation; Dark figure; Trans-territoriality; Rent-seeking from exaggeration.

1. Introduction

Both computer and mobile networks have exposed multiple vulnerabilities, played multiple roles in cybercrime, while the cybercriminals have been variably motivated [36]. There have been abundant discussions on the phenomenological issues revolving cybercrime. The purpose of this paper is to explore into crucial elements in the fight against cybercrime. The core question sought to answer is that of the ease ordinarily in the process of finding cybercrime, which includes a wide range of activities leading to punishment: reporting, detection, investigation, prosecution, fact-finding, proving, judicial decision-making, and finally conviction and enforcement of judicial judgment.

At this moment in time, the fight against cybercrime also requires improved understanding of the crucial elements. For several decades, many analysts have written about the features of cybercrime, and numerous aspects have been generalized with regards to the surveys, observation and thinking [58,67]. It is important to take such elements into account in different stages of the law enforcement process so as to improve the efficiency and effectiveness of the efforts.

Following this introduction, the paper will analyze the following crucial elements as special perpetrator-victim relationship, time elements, spatial elements, technological nature of cybercrime, complexity, costs, anonymity, hidden victims, concealment, trans-territoriality, and fast increase in recent four decades, which should be highlighted in strategic design of fight against cybercrime. The paper further analyzes the phenomenon of rent-seeking from the exaggeration of insecurity and cybercrime, which can be misinformation in this battle, before concluding the whole discussion.

2. Virtualized penetration-victimization interaction

Compared with traditional human-human model, the perpetrator-victim relationship in cybercrime is developed through Information and communications systems in a process of human-machine-human interaction. The perpetrator fulfils the first half of the interaction and the victim is imposed into the second half of the interaction. Namely, the victimization of victims of cybercrime also relates to information and communications systems. Victims are also users whose information is deposited in or published through information and communications systems, whose daily life or operation depends on the systems, or whose welfare is maintained through the systems. Like cybercriminals, they are also distributed over an unlimited area. In addition, in cases such as virus attacks, identity theft, and e-mail spamming, multiple victims can be involved in one incidence. Thousands or millions of users are also possible to be victimized in one case. Individual users usually have a lower awareness of cyber security than corporate users, and invest less money and time in maintaining and protecting the systems and less on updating their anti-virus software. Although individual users are more vulnerable to potential threats, their losses are usually neglected and underreported.

Computer networks are not so new, but the pervasive use of them is a recent development. The current generation of people accepts, and depends more on the computer and mobile networks than previous generations. There exists a clear-cut information generation within the information society. Because more young people use the Internet than the elderly do, it is natural that these youths are more likely to be victimized in cybercrime. Thus to some extent cybercrimes are offences of youths against youths. We do not find a sharp reduction of computer use with the increase in the age of young users. Therefore, it is to be expected that with the increase in age of the Internet users, more victims will also be found in future among older users.

Simultaneously, it is undeniable that with more and more organizations pursuing online businesses and other activities, the likelihood that these organizations will be victimized will also grow. In fact, the victims of the original offences against information and communications systems were mainly organizations. In the future, they will still be vulnerable to inside and outside attacks. One advantage these organizations have for protecting their information and communications systems is that they have a greater capacity than the individual users to afford the anti-virus, firewalls, other access-control mechanisms and for updating these mechanisms.

It is a trickier question when the online victims are more likely to be victimized in a "voluntary" or "active" manner. For example, the Nigerian 419 fraud victims may transfer a sum of money voluntarily to the perpetrators; victims of date rape may go to meet the potential criminals voluntarily; or users may voluntarily retrieve web pages that contain malicious codes, and so forth. Victims are also more likely to admit their "willingness" or "activeness" and less inclined to report the case.

Actual victimization in cybercrime can be more complex through the extension of victimization. For example, the senders of e-mail messages have adopted clever tricks in soliciting recipients. Opening the messages and the attachments is the first goal of the senders. Generally, they use ambiguous and false sender and subject columns, but ensure that there are valid contents (except messages spreading viruses) to show their offers and set their traps.

Unsolicited e-mail messages can have a broader influence on criminal phenomena, where the question is not only of victimization, but also one of conspiracy. Not only do e-mail communications become an offensive means by which the recipients are victimized, but these victims then serve as part of a conspiracy, for they are seduced to participate in criminal operations.

In the Internet environment, the most frequent victimization model begins from an exposing of victims to potential threats, which we can call the exposing-victimization model. With this model, the victim of unsolicited messages merely puts his/her e-mail address on the web pages, bulletin-board systems, uses it in the chat systems, or even simply transmits it through the Internet. The exposure is not necessarily a show-off. Rather, it is just a kind of presence on the Internet literally or digitally, something inevitable. Nevertheless, the exposing-victimization model at least implies that the senders of unsolicited messages could easily get the e-mail address in the same way as other Internet users do, without further efforts in collecting or harvesting these addresses.

In other cases, the senders of messages have a search process, and follow the searching-victimization model. Due to the large quantity of web pages and other Internet-related contents, the direct artificial collection of multiple e-mail addresses becomes inefficient. The senders (here we also imply address providers) utilize specialized software to harvest e-mail addresses from the Internet. This collecting process becomes automatic and efficient. The perpetrators have created the searching-victimization model in sending messages. Besides harvesting, they also use a dictionary attack and/or an automatic alphabetical permutation and combination to enumerate possible usernames in e-mail accounts. These methods can also be categorized into a searching process. For the senders, an e-mail account with a random word might not represent a specified person; but for the recipient, he/she is readily the victim of this unsolicited message with attachment.

The victimization of recipients of unsolicited messages happens without the appearance of the recipients in their e-mail account. The victimization means that their e-mail accounts are being spammed, whether they open their accounts or not. Under current the legal framework, the receiving of unsolicited messages is sufficient to constitute a victimization of the behaviour to be imposed punishment.

However, the victimization of unsolicited messages does not end at the initial victimization. The above-mentioned models could be called the first-level effects of unsolicited messages. Subsequently, the second-level effects are based on the initial victimization. There are possibly also two submodels: initial victimization-subsequent victimization model and initial victimization-conspiracy model.

The initial victimization - subsequent victimization model happens when the messages include viruses, fraudulent sales of goods, or falsified financing and banking services. The first-level victimization is being spammed, while the second-level victimization is being attacked or swindled.

Second-level victimization is not always fulfilled so simply. There is usually involved an initial victimization – exposing – searching - subsequent victimization process. In the case of the Nigerian 419 fraud, the recipients of the unsolicited messages were firstly victimized by receiving messages of this kind (being spammed). If they took a positive reaction to the messages, they were further exposing themselves to the senders. Upon receiving the recipients’ response, the senders further worked on the vulnerability of the recipients and the possibility of obtaining their property. The process of searching and exposing might be repeated a number of times. If the senders succeeded in obtaining the recipients’ property, the last stage of victimization would occur and the swindle would end.

The victimization-conspiracy model is realized when the messages include tax evasion services, sales of pirated software, sales of falsified documents, and so on. The recipients of such offers are firstly victimized by the unsolicited messages; and if they participating the illegal operations, they then become conspirators of the senders.

Because the recipients of the unsolicited messages inducing conspiracy in an illegal operation would expect to benefit from the cooperation with the senders, the senders are more likely to send attractive messages of the above kind. In fact, in Nigerian fraud, the senders are usually personating politicians who want to transfer property to the bank accounts of the recipients. As a result, the “conspirators” of money laundering are finally to be victimized in the trickery.

The phenomenon of unsolicited e-mail messages has further proved the low controllability or uncontrollability of the information-network environment. Any e-mail address is vulnerable to unsolicited messages that are sent to exposed accounts on the Internet or to a supposed account according to the dictionary. For the senders, both ways could be seen as a process of searching. For recipients, both ways could also be seen as a process of exposing. However, these searching and exposing processes have become more abundant and colourful in the Internet environment than during pre-Internet times.

The mere browsing of the web pages is the easiest method to get an e-mail account, but it is less efficient. The sender can also purchase millions of addresses of different interests of users from the specific vendors. At an inexpensive price, the buyer can conveniently reach a majority of these addresses. Besides, address harvesting becomes automatized and prevalent with the help of powerful software. Anyone with a mild computer and Internet knowledge has the ability to master the uncomplicated skills and subsequently collect thousands or millions of addresses with specific software, which can be downloaded from the Internet free of charge or with a small sum of payment.

The exposure of an e-mail account on the Internet is unavoidable, because the exposure is in so broad a sense that everything in the normal use of the account could be seen as an exposing process, including the sending and receiving of messages; publishing on web pages, chat rooms, and BBSes; providing account information to register in online services; or exposing nothing more than a coincidence with a phrase from a dictionary vocabulary; or merely a permutation and composition of letters and numbers so that the senders are also fabricated. In fact, exposure of a single e-mail account will not be so risky without the harvesting mechanism, because it is an inefficient way of picking up a single e-mail account from the Internet. However, it cannot be ignored because the e-mail account vendors could collect and transfer it in a dynamic process, and finally form a growing account database to maintain their business. The harvesting software and a dictionary attack undoubtedly deepen the victimization of the e-mail account holders.

In general, the exposed e-mail account might face double risks of being victimized: being picked up in a formal browsing of web pages and use of other Internet services; and being harvested and guessed. Compared with daily-used e-mail accounts without showing up on the web pages or other Internet services except merely sending and receiving messages, the published accounts are more likely to be victimized. Therefore, it seems more likely that it is the process of harvesting rather than that of guessing is the one that the vendors of the database of e-mail accounts and senders of unsolicited messages feed on. As a result, the double risks of exposed e-mail accounts are in fact unbalanced risks: the risk of being victimized by collectors and harvesters is far more serious than the threats of the guessers.

Unsolicited messages provide e-mail users with several different choices, either legitimate or illegitimate, either to conspire or to be further victimized by attached viruses or pre-established fraud traps. The majority of messages granted recipients two alternatives: to conspire in tax evasion, or to be damaged by viruses.

In the case of conspiracy in tax evasion, the senders always provide valid contact methods to induce the recipients to participate in illegitimate activities. These offers seemingly aim to establish a relationship between service provider and clients. Nevertheless, the true effect is that they form a conspiracy. The recipients have to react actively before they become conspirators in tax evasion schemes. The process might involve repeated exchange of e-mail after the initial unsolicited messages. Under these circumstances, the unsolicited messages might be transformed into literally valuable (but morally wrong and legally prohibited) information. Thus, the recipients might be less averse to such messages. Such messages become the means of communication for the trespassers and criminals, hence posing great threats to social-control attempts to frustrate illegal activities.

In the case of viruses attack, the senders exploited social engineering to induce recipients to open the messages and subsequently the attachments, by blurring the sender and subject columns and falsifying the message contents and name of the attached files. These messages do not require replies from the recipients before they cause damage. They are also dangerous for the recipients in the sense that they are harming the recipients' hardware and software, wasting the labour force, and hindering the business.

3. Synchronized penetration in cybercrime

All offences happen in relation to a certain time. The networks make a more efficient use of time, either in positive social actions or in negative social actions. A single cybercrime can be completed in a very short time, say, seconds or minutes. The simplest example is to modify or destruct data in a hard disk. The more complicated example is the possibility of transferring the U. K.'s total currency reserve in 15 minutes to another country [31]. General cybercriminal offences can involve tremendous information transmission in a relevantly short period.

However, preparation for some kinds of cybercrime may be time-consuming, usually taking several days, weeks or even months. It depends on the attacks projected, the complexity of the process, and the security technology of the targeted users. The more sophisticated the perpetration is, the more time is needed for preparation and processing. The more sophisticated the security measures are, the more time is needed for overcoming them.

Many offences are committed in a particular natural time or social time. Natural time is the time-span depending on the natural cycle, for example, four seasons and 12 months of a year, seven days of a week, twenty-four hours of a day, day and night, etc. Social time is the time span depending on the social cycle, for example, work time and spare time, holidays, etc. Circumstances are particular time-spans accompanied by natural events, such as wind, snow, rain, etc., or social events, such as war, riot, strike, demonstration, etc.

In the traditional crime of bank robbery, robbers have generally to act when the bank is open, when money is in the safe, when money is being transferred by special vehicles. It is not a prerequisite for cybercrime to depend so much on time. In principle, electronic cash can be "stolen or robbed" at any time, whether it is work time or not.

Many traditional offences are environmentally or weather dependent. In the case of cybercrimes, the environment and weather become less important. For example, in traditional larceny, when a thief walks in rainy weather, the footprint may soon be eliminated by water, but the footprint may be left if it is in the snow; the wind may conceal the sound of a footstep, and it may be more difficult to see the thief in the dark than on a clear moonlight night. In the environment of cyberspace, the element of weather is nearly irrelevant, that is, cybercrimes are an all-weather business. In whatever kind of weather, cybercriminals can sit at a computer and perpetrate whatever kind of activity without fear that victims or the third parties will discover him in person.

Cybercrime can cross time-zones, so that the "time" in a day, measured by the criterion of law enforcement, is not so relevant in the offence. Traditional offences may be committed in different periods of the day, for example, stealing when it is dark, burglarizing when the house-owner is at work, etc. Online illegal obtaining of information and money may not be time-limited. However, due to strict supervision and the monitoring of online activities, the perpetrators may have to avoid the work time.

Once successful, attacks may continue for a long time, for instance, for several weeks or for several months. In the case of pure illegal access and the obtaining of information from computers, the victim can hardly find the intrusion in the subsequent months. The intrusion may be repeated before the loopholes are fixed. In addition, influences of some kind of viruses on whole networks may last for several years. Once created, viruses can never be annihilated and prevented from spreading. Although old viruses may become less harmful due to the use of anti-virus, the less protected computers can still be infected in subsequent years. Another example of continuing cybercrime is the Nigerian 419 fraud, which has been prevalent for several decades and is still a big threat to Internet users.

Malicious programmes, frauds and some other cybercriminal tricks, once they have emerged, may be analogous to natural viruses or bacteria. They exist independently despite people's use of anti-viruses, which are like an immunity injection for human bodies. As viruses or bacteria may infect those for whom the injection has failed to take, the failure of anti-viruses may reveal the vulnerability of the systems. The attack happens wherever there is a security loophole.

4. Spatial elements in cybercrime

Like traditional crimes, cybercrimes are also more or less related to the element of space. The possibility of the trans-territoriality of individual cases is high.

The phenomenon of cybercrime is distributed everywhere. In some cases, offences are committed in such a way that the activities take place in a distributed manner. The frequencies of these cases are different in various regions and countries. The objective description of the global situation proves that though cybercrime is characterized by its universality, it is undeniable that cybercrime cases are rare in some countries. For example in Finland, according to Miettinen, from 1980 to the time his study was published, the officially-investigated hacking cases were only 10-15 in number [45]. Although hacking cases involving one or two million dollars of losses also existed, the frequency and severity of the cases were less comparable with cases that happened in countries such as the U. S. In West European countries, cybercrime is also less serious than in the East European transition countries.

Definitely, cybercrimes also leave some kind of traces in digital form and can be used as clues for a traceback. However, we find that cybercriminals are less anxious about traces of this kind than about the risks of being exposed in person. The straightforward example is a person who will dare to intrude into a computer in a neighbouring room through the LAN or WLAN, but not dare to enter the neighbouring room without permission to gaze at the computer screen, not to mention operating that computer without permission. Trans-national cybercriminals are less discouraged from engaging in these activities by the deterrence of law enforcement.

5. Technological involvement

In the new millennium, the information economy is a popular expression used by entrepreneurs, while cybercrime is a popular expression used about the criminals. Many scholars have recognized the intensified technological involvement in cybercrime (for example [9,11,30,39,48,64,70]). In all cybercrimes, computers and the Internet are used as tools. Even if what is in question is an attack where computers or networks, or information is targeted, the necessary tools are still computers and the Internet, without which the offence may fall into the traditional offences, and cannot be classified as cybercrimes. However, technological involvement is a necessary but not sufficient condition. Illegally assembling computers with market traded computer parts can hardly be a cybercrime. Yet, illegally manufacturing computer chips can be. Definitely, if traditional forces and technological means are combined in a certain offence, both cybercrime and traditional offence can run together. For example, a bank employee may be abducted and forced to reveal the IDs and passwords. The combined use of these means is not rare in practice.

Certainly, the computer may not be the only tool in a certain cybercrime. For example, wireless networks and mobile networks provide particularly complicated ways of making a command to launch an attack.

The extent of technological involvement is different in various cybercrimes, from simply cracking a less complex password to controlling thousands of bots all over the world to launch distributed denial of service attacks. The situation is, regardless of whether straightforward or sophisticated techniques or instruments are used in illegal activities, the damage can always be substantial. Although the overall losses of computer misuse are difficult to calculate, the losses of a single victim may be overwhelming, particularly when an individual does not keep separate back-ups. An attack, even by a straightforward technique, can also result in serious consequences in considering the various detailed situations of victims.

In cybercrimes, in addition to the possibility of manoeuvring multiple computers, the available tools, means and functions are also numerous. In fact, much malicious software can be downloaded from the Internet. Many hacking techniques can be learned online. There are opportunities to purchase a malicious programme from the Internet as well.

6. The sophistication of cybercriminal activities

The Internet allows for the communicating and planning of criminal activities in more different ways than in even the recent past. The Internet also accommodates exchange of cybercrime methods free of charge, or provides sales of malicious programmes [4]. Advanced criminal mechanisms enable the attackers to avoid prosecution or complicate investigations in a straightforward manner [61]. This further enhances their universality and concealment, making law enforcement more and more impossible.

Furthermore, imagine the time when there were only 20,000 computers connected to the Internet globally, Stoll (1988) described the process to trace the break-ins by a persistent computer intruder attacking Lawrence Berkeley Laboratory (LBL). The traceback took nearly a year of work apart from requiring the cooperation of many organizations including the U. S. FBI and the German Federal Criminal Police Office, during which the intruders continued their activities against 450 computers and successfully gained access to more than thirty [65]. Even then because of the complexity of the cyber environment, investigation of cybercrime cases was extremely time-consuming. In comparison with cases affecting thousands or millions of computers, the difficulties in investigating these relatively trivial cases poses the question of how the prosecution of a major case is possible.

Johnson has discussed digital forensic evidence on both national and international levels, the challenge posed by offences of online pornography, encrypted illegal materials, cyber terrorism, cyber crimes against children, and the exploitation of computer viruses in extortion schemes. He found that the process of searching digital documents was extraordinarily difficult, due to the capacity of rapid transmission, storage in remote machines, encryption, or the use of other concealment methods [30].

The Internet being a vulnerable infrastructure, all the individual and institutional Internet users are exposed to similar threats of becoming victims of cybercrime. In practice, all cybercrimes are more or less committed through technological means. Malicious programmes and anti-viruses are "weapons" in information and communications systems. Malicious programmes are usually designed and disseminated without rewards, being uncommercialized and unsystematic. Anti-viruses are designed and sold as commodities. Both of them are products of labour, but with a different use: the former being offensive weapons, the latter being defensive weapons.

McAfee has summarized tools and their functions in cybercrime [40]. These tools are used not only to access confidential information, but also to conceal traces, and prevent normal functioning. Most of these tools can be downloaded from the Internet free of charge or at inexpensive prices. It is especially easy to search and obtain such a programme from the Internet as freeware or shareware using a search engine. Many tutorials are furthermore prepared for non-professionals to study them systematically from primary level.

Compared with malicious programmes, the sources of preventive programmes are fewer in number and more expensive on the market. To search such a programme on the Internet turns out to be more difficult than obtaining are free of charge. The usual results are that the links are redirected to a trial version with limited functions or a full version with payment instructions. The incentives for not revealing such programmes are profits, compared with the incentives for causing broader and larger damage and gaining fame by the revelation of malicious programmes. These cases are akin to cases of copyrights and their infringement.

Both elements can be simplified because of the abundant opportunities for abuse of information and communications systems. In fact, many practical cases have shown that rather than depending on sophisticated technologies and overcoming complicated processes, the perpetrators simply exploit the opportunities at hand. An offence primarily engenders by opportunity, should not be measured by the sophistication of techniques and the complexity of the processes involved.

7. The expenses, benefits and losses of cybercrime

Although much literature dealing with "the costs of crime" has been written by economists, statisticians, jurists, and sociologists, the practical estimate of the costs of one single offence or the whole criminal phenomenon has proved impossible to work out. However, the costs of crime can roughly include direct and indirect costs, physical and psychological costs, and both the costs before the incident and after the incident. There have been efforts to quantify the losses of computer crime, for example [73], or measuring the size of the problem [23]. In respect of the losses caused by cybercrime, it is overall so expensive that no other criminal activity can compare with it. Sometimes, the "losses" of one offence may not necessarily be a pure social cost. Some of the wealth may be transferred from the victim to the offender. Generally, the more the offender obtains physically, the more the victim loses. In some other cases where the offender does not acquire substantial property, mere "losses" of a victim's money or health satisfy the offender's psychological needs. In both cases, the offender has expected benefits. Again, the more the victim loses or the more seriously the victim is hurt, the more the offender is satisfied psychologically.

Monetary losses caused by crimes, particularly by cybercrimes, are thus difficult to calculate. Direct measurements being unavailable, only some important references can be used to indicate the extent of these losses.

As a first reference, because individuals and businesses have to invest heavily in information security and have to change their behaviour to reduce the probability of being victimized [24], spending on cyber security services and products constitutes, for example, a significant part of the losses brought about by the threats of cybercrime. Without cybercrime, The ICT industries do not require to invest specifically in security protection. In the meanwhile, investment on security protection does not increase productivity. Presently, this expense becomes a necessary part of their ordinary inputs.

The second reference is that losses in individual cases provide a more direct impression. Daler and co-workers reported that the average loss obtaining in a cybercrime case is around 400,000 dollars, as compared with the average take in an old-fashioned bank robbery of 6,000 dollars [15]. The CCIPS web site publishes a list of cybercrime cases prosecuted in the U. S. in recent years. It is obvious that once the cases involve losses, the amount will be large (definitely, there are also cases not involving any monetary loss) [7]. Calculating the 115 cases prosecuted during March 1998 through to May 2006, the lowest single loss was 5,000 dollars, and the highest was 80 million dollars. The average loss in these cases was 1.27 million dollars [35]. The losses involved in single cases differ from each other.

The third reference can be obtained from various cybercrime surveys, each of which provides some information about the situation of the respondents. For example, the annually operated CSI survey on 700 US computer security practitioners in corporations, government agencies, financial institutions, medical institutions and universities, found that the reported average financial losses resulting from security breaches are 204,000 dollars per respondent. The total losses for 639 survey respondents came to exactly over 130 million dollars [14].

Accurately calculating the losses of cybercriminal offences is a task of some sophistication [69]. Cybercrime is a comparatively easy business, but the deterrence, in its turn, is far from easy. Notwithstanding the fact that the whole world is actively combating cybercrime, the number of cybercrimes is still on the rise and their costs are increasing exponentially [13]. In 2005, estimation of losses reached 400 billion dollars [40]. The meaning of this number from the year 2005 may be well understood if we compare it with the 9/11 attacks that cost New York City at least 17 billion dollars. Further, it may be pointed out that the forecast for the effect of terrorism in general, is a reduction of 0.25 percent of the world economy's growth rate -an impact of around 75 billion dollars [16]. If such comparisons are used in measurements, worldwide overall cybercrimes is bleeding the economy of nearly 24 times the sum of the 9/11 attack losses. In addition, companies are investing heavily in a variety of security technologies and insurance [61]. This is not unrealistic, if we recall that the International Monetary Fund June 2002 Global Financial Stability Report reflects, in a conservative estimate, the total insured losses for 9/11 of around 44 billion dollars [29].

Besides the direct cost, Loeb has estimated that breaches of confidence can make companies lose more than 5 percent of their market value on average [37]. A survey by Telang and Wattal analysed the economic impact on 18 software suppliers and found that announcing vulnerability in one of these companies' products caused a 0.6 percent fall in its stock price, or an 860 million dollars fall in the company's value [66].

Immeasurable are the losses of confidential information on state security, governmental reputation and diplomatic relationships. In general, what makes the situation worse is not only that cybercrime is expensive, but also that the costs are rapidly increasing. Only if it reaches saturation point, can the speed of development become stable or commence to decrease. Furthermore, in the "competition" between the criminals and law enforcement, it is obvious that the former are more efficient in obtaining new technologies than the latter [8].

The above analysis concentrates on the general impact of cybercrime on society. A special issue requiring clarification is that of the impact of cybercrime on individual victims, comparing a pensioner and a millionaire both of whom are undergoing 100 euros of losses in a cash card fraud. The direct suffering of the former is definitely far more severe than that of the latter. Criminal justice, equally protecting the poor and the wealthy, may reasonably be considered inefficient in equally treating every euro value of property belonging to every person. In addition, traditional crime can be lethal to natural persons, but has a less severe threat to legal persons in general. However, more and more businesses have considered cybercrime more likely to happen, and more harmful than physical crimes. This is a natural result of increasing importance of information for enterprises and increasing threats of cybercrime to information security.

8. The anonymity of the perpetrators of cybercrime

Communicating anonymously is a great characteristic of the Internet environment. In using the Internet, anonymity can be kept from the beginning to the end thanks to cryptographic techniques such as that used in blockchain. First, anonymous access to the Internet poses the most serious threat. In many countries, one of the most important forms of using the Internet is realized through cyber cafés or libraries, where anonymous users can access many of the online services. Definitely, there exist different situations in different countries. Compared with Finland where there are few cyber cafés in towns and cities, the cyber cafés in China have become the "third space" of school-aged juveniles besides home and school. The facilities and services in academic or public libraries are far less convenient for users than those in cyber cafés managed by private firms. An increasing number of hacking cases involving the Internet or Internet users are committed or conspired in cyber cafés.

Secondly, anonymous subscription to the Internet services raises the difficulty of identifying users. The personal information provided for the registration of an e-mail account, the name and address of e-mail messages, and the authors' information in Usenet, etc., can all be fabricated. Keeping identity anonymous is favourable for the protection of users from victimization, but it also favours the hiding of perpetrators from being traced.

Thirdly, users can keep their identity anonymous in the process of online communications. There are also mechanisms for keeping complete anonymity by which one user can send messages to other users, and then the messages are transmitted to the final target, such as newsgroup, e-mail list, or a single e-mail account. What makes it more complex is that in the mechanisms the intermediary can only be a programme and may be in another jurisdiction [32]. This also reminds us that there exists the possibility of numerous transmitting points, by which messages are transmitted from one terminal to the next terminal, from that to the next in line, and so on, until the message reached the destination. Tracing this transmitting process is theoretically possible. During the tracing process, the investigation is exactly the contrary to the process of transmission. Each time, the investigator can trace back one point.

It is likely that all points are identifiable. Nevertheless, as long as there is an unexpected element at any point, the tracing chain can be disrupted without reaching the original source.

According to National Police Agency of Japan, the possible examples include that the victim has no record of the Internet Protocol (IP) address; ISPs do not keep suitable records; hackers alter the logs; or some points are located in countries that have not criminalized hacking [50]. Even if all the work of traceback is fulfilled, the actual value of this work may be discounted in a judicial process because of different locations and thus diversified jurisdictions.

Fourthly, the specific service or software can play further roles in hiding users. Cybercriminals usually establish anonymizers, which are systems particularly designed to invalidate technical identification of the source of communications. In fact, this kind of service or software can also be conveniently obtained free of charge or at an inexpensive price from the Internet. Everyone who is online can get access to these tools and services. Such software is likely to be replicated and spread unlimitedly, creating a bigger population of hidden users who potentially threaten the security of information and communications systems.

Although the anonymity of cybercriminals poses a series of questions, it is still the core of the “perfect environment” for the criminals; yet it is at the same time welcomed by Internet users. People are constantly concerned that without online anonymity, it could be impossible to guarantee fundamental rights [50]. Philip warned that anonymity can provide users with the bravery to do the disgraceful and occasionally even resort to illicit activities [53].

9. Concealed victimization

Cybercriminals have a greater advantage than most of the traditional criminals in respect of the low probability of arrest and conviction. Many scholars have mentioned this characteristic of cybercrime. Hatcher et al. have pointed out that many cybercrimes are not reported [26]. The term “dark figure”, used by criminologists to refer to unreported or unrecorded crime has been applied to denote undiscovered cybercrimes [69]. Many intrusions are not detected for a variety of reasons. Cybercrimes can well be described as hidden crimes.

At the same time, victims of cybercrime are willing to be hidden victims [12]. The usual “motives for silence” concerning victimization may fall into one of the following categories: 1. The idea that the victimization is not worth the mobilization of justice; 2. Involvement; 3. Pressures of fear; 4. The uneasy accessibility of police and court; and 5. The ignorance of events by the police [54].

In sketching the victim decision-making, Greenberg and Ruback have established a three-stage model: the victim judges whether the event is a crime, evaluates its seriousness and decides what to do [19,25]. Before these stages, one stage that is more important should be added, that is, whether the victim knows the event. If this is the case, the reporting of cybercrime may remain at a lower level, because cybercrime is invisible and difficult to discover; it is more difficult for the victim to judge whether the event is a crime and to estimate the losses; and the victim has less knowledge about whether there is an agency to report the crime. The limited reporting of the cybercrime has been noted by Parker and Nycum [51], who studied the invisibility of computer crime. At present, the Internet’s virtual environment has made the situation still worse. Fortunate progress in proving material evidences in traditional crimes was made in late 1980s when DNA tests were first introduced [34]. However, digital evidence in computer crimes is immune from such high-technological testing measures. The invisibility of cybercrimes is based on several elements, either technological or human [69]. Sometimes, the simple reason is that the victims are not willing to report, or even do not know where to report the case [56]. The documented reasons for the reluctance to take legal actions are mainly fear of adverse publicity, public embarrassment or loss of goodwill, loss of investor or public confidence, resulting economic consequences such as the panic effect that this information would create on their stock prices [6,22,43,55]. The UN suggested that these elements have a significant impact on the detection of cybercrime [69].

Yet there are other reasons for the victim to keep silence. While many people are active in maintaining their interests and rights, some people view victimization as their own failure in life and career and are not willing to reveal the fact of their failure to any individuals and institutions, so as not to make public their own weakness.

Therefore, it is inevitable that the rate of unknown instances of cybercrimes has increased as a result. The CSI summarized the reasons why the U. S. organizations did not report intrusions to law-enforcement agencies, including unawareness of law-enforcement interest, a civil remedy seeming the best course, computer would use to their advantage, and negative publicity would hurt the image of their stock [14]. This survey has indicated the percentages of respondents identifying each stated reason as being very important in their decision not to report computer intrusion. At the same time, it is worth noting that the reasons are subject to changes in each annual survey.

10. Concealed perpetration

Mitchell and Banker have concluded that there are four characteristics in which cybercrimes are different from traditional crimes, that is to say, difficulties in detection, limited reporting, jurisdictional complexities, and resource constraint [47]. All these four aspects fall under the broad characteristic of concealment. The concealment of cybercrimes has been brought about by other technological and human elements [9,11,30,39,48,64,70].

Most of traditional offences are highly visible due to apparent depredations, presence of witnesses, and so on. There are also traditional crimes that occur in private places and become less visible [72]. Unlike traditional threats where criminals are physically present at the crime scene, cybercriminals are usually not present at the crime scene thus making apprehension difficult [62]. In information and communications systems, executing a command to delete files does not mean that the files are permanently deleted. What happens is merely that files are hidden due to a change in file names so that the files can be recovered, except when a secure-eraser programme is in use. Skilful criminals can disable this kind of security mechanism, and conceal the data that might possible be taken as evidence in prosecution.

Technological advances have both a positive impact on businesses and a negative impact on law enforcement [28]. For example, in the DrinkOrDie case, the online software piracy group concealed its actions by various security measures: exchanging e-mails via private mail server using encryption; using a nickname to identify members, and communicating about group business only in closed, invite-only IRC channels; the FTP sites, where tens of thousands of pirated software, game, movie, and music titles were deposited, were secured by particular authentication mechanisms (U. S. Department of Justice, Press release, 17 May 2002). On the other hand, the available technological solutions have not completely met the requirement of data collection, log analysis, and Internet protocol tracing [2]. There is also the necessity for law-enforcement agencies to recruit personnel with “electrical engineering and computer-science backgrounds” [21].

Concealment of crimes has important economic effects. Stanley stated that concealment of crime can decrease the incentives not to perpetrate, and increase the costs of law enforcement [63]. Concealment of cybercrime demonstrates the low probability of punishment. In the U. S., only one in 100 cases was detected, one in 8 prosecuted, while only one in 33 prosecuted cybercrimes resulted in a prison sentence. That is to say, the likelihood that a cybercriminal would be put into prison was a one in 26,400 chance [15], as compared with the likelihood of imprisonment in traditional bank robbery a one in three chance. Law-enforcement agencies found that a majority of cybercrimes never reached the criminal-justice system. Even in the relatively few cases where a crime was reported, most often the criminal's identity was never discovered. As a consequence, as Radzinowicz and King pointed out that the computation of probability is as appropriate to the commission of crime as to lots of other activities [54]. Given other elements constant, if cybercrime is more concealed than other offences, the potential perpetrators are more motivated to take illegal actions on the Internet, and thus more offenders of traditional crime will be prepared to migrate to cyberspace.

11. The trans-territoriality of cybercrime coverage

Free flow of information from one country to another is a goal of information and communications systems, but trans-border flow is not free. The trans-border information flux is accompanied by risks of crime of a similar nature. In any country, the court must have jurisdiction over the person or the subject-matter of a lawsuit. This works well with the current set-up of law-enforcement agencies that are territorial and are operating in different villages, towns, districts, cities, counties, states or provinces, or national boundaries. Nevertheless, unauthorized access to information and communications systems can be accomplished from virtually anywhere on the networks. In fact, some of the cases prosecuted have been of this nature.

The sphere of legal jurisdiction makes the cybercrime enforcement more complicated [33]. Smith et al. concluded that the trans-national dimension of cybercrime posed four formidable challenges for prosecutors, who have to determine whether the conduct in question is criminal in their own jurisdiction, collect sufficient evidence to mobilize the law, identify the perpetrator, and determine his or her location, and decide whether to leave the matter to the local authorities or to extradite the offender [60].

Sinrod and Reilly have pointed out that although some international organizations are examining cooperative mechanisms in the field of fighting against cybercrime, many of their members are slow in recognizing the urgency of the situation [59].

The elimination of borders favours inter-jurisdictional mobility of crime. Due to the actual difficulty in establishing jurisdiction, even if a certain offence is detected, it is still uncertain whether the way can easily lead to punishment. Reasonably, suggestions have been made to incorporate cyberspace into various jurisdictional frameworks. Nonetheless, this needs a great deal of time, agreement, and co-operation between countries, which are still struggling to take common actions.

Finally, it is worth noting that trans-national cases only constitute a minor part of cybercrime [35]. No certain conclusion can be drawn because it is possible that trans-national offences are not as prevalent as scholars have assumed. On the other hand, it is difficult to reveal these offences for reasons that scholars have laid bare. Or, it may be, that it is simply law enforcement does not put sufficient emphasis on these offences. Before credible data are available to give an answer to this question, we have certain reasons to claim that trans-national offences have sometimes of a dual nature: they do not appear as prevalent as domestic offences, but they are more difficult to detect and convict. In addition, because the investigation of trans-national offences is more expensive and time-consuming, law enforcement will not give more priorities to these offences than to cases that have happened “close to home”.

12. The rampancy of cybercriminal phenomena

On the computer age, Bequai said, the computer was a gigantic calculator enabling people to gain large quantity of data by pressing a button [5]. When the computers are connected as a colossal network, “buttons” are used not only to acquire and transmit data, but also to replace some of the traditional interpersonal communications and social interactions. Collin explained the sense of the virtual world, being “symbolic - true, false, binary, metaphoric representations of information - that place in which computer programmes function and data moves” [10]. Cyberspace has developed into a stockroom of the wealth and power of the information age [38]. The pervasive application of ICT can be regarded as a magnitude change of the contemporary society. It poses new challenges to the traditional conception and system from many aspects, and it changes the routine activities of a large population of the members of society. This change, among other effects, will benefit the disorganization of the traditional social structure and thus increase the presence of motivated perpetrators and the exposure of their victims. As a phenomenon long existing in society, crime has transformed its forms and grown steadily in different historical periods. Criminal phenomena have always gone beyond the law. New forms of crime will inevitably emerge from a continually developing society, while the law is not ready to guard against them. The requirement for punishing crime requires a revision of criminal legislation and a renovation of criminal justice. The persistent extension of the ranges of crime can but result in the constant extension of the regulating domain of criminal law.

People longed for the industrial society in which their economic situation would be improved, the education level enhanced, consciousness civilized and traditional crime decreased. However, not only has traditional crime not decreased, but also white-collar crime came into being. Where white-collar crime was the offspring of an industrialized civilization, cybercrime concomitantly grew in hand with an informationized civilization. The unprecedented combination of crime and computer creates a stage of anti-productivity, undermining the magnificent prospects for high technology. Criminals abuse the conditions of the emerging market and technologies.

The rise and prevalence of the Internet has become the prominent intervention element in the development of cybercrime in the recent decade. On the Internet, exist universal contradiction and contention, use and abuse, defence and offence, ethic and deviance, fact and falsification, order and disorder. The powerful software and hardware that enable people to work more effectively is difficult to operate securely [1]. Speedy technological evolution makes the vendors concentrate more of their time on the market, and less time on security features [52]. Although computers and networks are at present protected by various means, the emerging vulnerabilities are inevitably increasing.

All these considerations concerning criminal phenomena in the background of high-technology development does not imply that it is the technology that brings about more crimes. Nevertheless, we cannot deny the element that the adoption of the new technology may make the crimes more profitable, and less risky [15]. Even worse, the criminal will tend to repeat his or her criminal acts-- especially when there is little chance of being caught or convicted. Consequently, cybercrime would pave the safest way to illegal profit, considering the ease with which it can be committed and the negligible chances of imprisonment [15].

If we consider that many devices and facilities of the today's society are network-connected today, these trends can be more detailed and concrete in reality [18]. For example, according to Chris Mitchell, a modern car contains networks of communicating devices, which control most aspects of a car's operation, including its brakes, gears, throttle, and engine management [46]. Functionality often also includes external connectivity, e.g. including mobile telephony. This gives rise to a large and varied attack surface, including the following elements. In the US, the mandatory Onboard Diagnostics Unit (OBD-II) port provides direct access to the vehicle's internal network. User-upgradeable systems (e.g. audio players) are routinely connected to internal networks. Wireless devices (e.g. Bluetooth) are also connected to internal networks. Finally, and most seriously, remote telematics systems (for safety, diagnostics, and anti-theft) provide continuous connectivity via mobile phone networks. A team performed experiments using two cars purchased specifically for purpose. They observed that the car's internal CAN bus has little security – any compromised component can impersonate any other component. There are many other security issues. They demonstrated remote attacks on a car via a broad range of attack vectors, including: mechanic's tools, CD players, Bluetooth and mobile telephony. To perform a mobile phone based remote attack, they reverse-engineered the telematics protocol and used buffer overflow vulnerability in the car gateway to take over the car telematics unit. This attacks works completely 'blind', i.e. without listening to responses from vehicle. Building on this attack they demonstrated the ability to compromise internal vehicle systems, and thereby systematically control the car's engine, brakes, lights, instruments, radio, and locks. The attack could be exploited for theft and surveillance [46]. This remind us that, most of today's vehicles, such as motor vehicles (motorcycles, cars, trucks, buses), railed vehicles (trains, trams), watercraft (ships, boats), aircraft and spacecraft, are more or less assisted by network services and are all vulnerable to various potential cyber attacks. Therefore, there is the possibility that cost of cybercrime can still grow significantly in near future.

13. Rent-seeking from the exaggeration of insecurity

The social reaction to and impression on cybercrime are broadly diversified. The general public who are not unfortunate enough to experience or witness real life offences usually rely on the reports of the mass media. While the mass media have their own interests other than maintaining a peaceful and secure daily life, the texts, graphics, audio and video files they compose and create can distort criminal incidents. Some characteristic ways of reporting computer crime have been misleading, even though they play roles in reinforcing the public consciousness of security [49].

The tendency to dramaticize and mystify offences that the general public do not often hear about and see stems from the benefits gained by the mass media from their show-off through selective reports. They choose to broadcast what they consider capable of attracting an audience, while at the same time they keep a silence about events in which they have less interest. The most important principle of the media is to be authentic. However, their authenticity is built on selective reports. First identified by Gordon Tullock [68], rent-seeking finds its way into cyberspace. Anderson has contributed to the study of exaggeration of cyber insecurity by pointing out in his paper that many interest groups would unavoidably engage in manoeuvring the truth of the cyber insecurity to benefit from the scared market [3].

The players may include the mass media, the security engineering community, security professionals, police officers and even professors [3]. Schneier has criticized the fact that software vendors may have an incentive to exaggerate insecurity [57]. In fact, Hoo has suggested that straightforward, cheap measures are much more worthwhile than large projects that many security vendors prefer to sell [27]. There is definitely a problem that many organizational users leave their computers on and online the whole night after work, many without complex access control. Broadband networks provide a convenience for individual and organization users to keep online 24 hours a day, and seven days a week. Sometimes those who are their contacts can even find their online status in the chat or e-mail systems. The 24-hour-online model is practically more risky than a dial-up service in terms of longer online time.

Doing this research, I have found that many manufacturers of computer hardware and software also have a tendency to provide a darker picture to users when presenting the problem of cyber security. This becomes easier to understand when we recall that these manufacturers are striving to survive the growing threats of consumers' awareness against the market of their products. In order not to subject them to product liability, they have to adopt a preparatory stance of impressing the users and judicial organs that the reason for cyber attacks lies not in the defects of their products but in the malicious motives of the perpetrators.

14. Conclusions

The development of cybercrime necessitates a timely update of the law, as some countries have done. However, it seems that the laws implemented are inadequate for effectively addressing the problem [71]. An example of this aspect can be found in the definition of fraud in U. K. The traditional fraud definition required that a person but not a computer be deceived [15]. Thus, the application of fraud provisions has depended on whether a person has also been deceived. These authors have mentioned that only in other countries, not the U.K. have the provisions on fraud been interpreted more broadly.

According to the McConnell International [41], only 31 percent of the countries surveyed had substantially or fully updated their laws, 15 percent partially updated, while more than half of the countries had no updated laws. According to the principle of legality, the absence of a law punishing cybercrime sets the deterrent probability at zero, while the actual punishment is also zero. This being the situation, the expected utility of the offender equals the utility when he or she is undetected. By recognizing this benefit, the potential perpetrators will have a greater incentive to commit cybercrime than other offences.

As the conclusions of McConnell International have demonstrated, light punishments create limited deterrence [41]. The possible reason why creating a virus carries lighter penalties than marijuana offences may be due to the elasticity of these two kinds of crime from the economists' point of view [42]. Unlike the marijuana offences that are inelastic, cybercrime is more elastic. Tougher punishment for drug crime will be less effective than for cybercrime. However, considering the marginal deterrence when the effect of punishment is too weak to stop cybercrime, this definitely does not deter, either. Lack of a certain degree of severity in punishment will not prevent potential criminals from committing the crimes they are planning, because even if they are probably caught, their expected benefit will still be higher than the expected cost. It is the marginal deterrence of the punishment but not the elasticity of the crime that is working.

However, at the same time, methods adopted in some countries cannot be completely explained by the above theory. Take the example of the application of long-term imprisonment for offences with a low detection probability. The expenses of the long-term imprisonment are quite huge. Thus, it may be said that under these circumstances, governmental investment is insufficient when the emphasis is put on punishment, and detection is ignored. This relates to the value orientation of the government.

Some other countries completely violate the principle of rational choice. They seem to find it difficult to afford adequate funding for detection, conviction, and enforcing punishment, while on the other hand they have established a cyber police, employing huge police forces. The tasks of these cyber police include detection and evidence collection, as well as cybercrime prevention with techniques and human resources, forming a "cyber information dam". The expense is also huge. As Dnes pointed out, it is of very poor value to increase the probability of conviction through employing more police officers [17].

In these countries, the concerns about the privacy of individuals have to give way to national security and the maintenance of social order. This means that in the information age, the public organs receive ever greater powers of surveillance and interception. Since the 1990s, the terrorists have frequently launched attacks; and individualism is gradually being submerged by the voice of national interests and international co-operation. The role of punishment in the deterrence of crime is undoubtedly unearthed. Whether in poor or wealthy countries, severe punishment is being used universally for cybercrime. This can be explained as decreasing the expected benefits of cybercrime while increasing the expected costs, forcing the offenders to give up committing the offences and to select instead legal activities. This implies that the means the modern countries take to decrease crime are direct prevention, plus increasing detection probability and increasing punishment severity.

Nevertheless, the following elements deserve further consideration. First, it remains a doubtful question as to whether the information dam can effectively control the information flood. The filtering and blocking of information is expensive and ineffective. As a substitute for severe punishment, it is either a necessary waste of democracy (compared with over-criminalization), or a necessary limit to democracy (compared with information freedom). In order for cyber security to be maintained, the private sectors and the public authorities should cooperate to strengthen the legal frameworks for cyber security [41].

Secondly, a surer answer can be provided to the question of whether severe punishment is cheap. There have been hundreds of studies done concerning the cost of the death penalty, proving that the death sentence is expensive as well as being easy to execute the innocent. These have become common-sense reasons for repealing the death penalty. The cost of imprisonment is also high. Because the cost of severe punishment is costed differently in different countries, the legislature and law enforcement have a different tendency in implementing various degrees of severity in implementing punishments, which can bring about further jurisdictional problems.

Finally, what should be researched is whether severe punishment is effective. Given that the probability of detection remains extraordinarily low, and that there is no appropriate approach to increase it, a severe punishment again runs up against a limitation. A severe punishment to some extent requires the support of the probability of detection. If not, it loses the basis on which it exists and delivers little deterrence at all.

Cybercrime differs from traditional crimes in its universality, anonymity, concealment, and complexities. While quantitative evaluation of cybercrime has proved difficult, the fight against cybercrime has become a big burden for companies. Because of difficulties in detection, investigation, and conviction, the dark figure of cybercrime remains high. The harsher penalties should be applied to pursue effective deterrence, but in themselves they do not serve protection.

In effect, we are still repeating Radzinowicz and King's dilemma: the perpetrator may escape detection, the detected perpetrator may escape arrest, the arrested perpetrator may not be brought to book due to lack of evidence, the perpetrator brought to book may be released because his innocent context or trivial offence, the prosecuted perpetrator may escape conviction, and the convicted perpetrator may only be imposed a light penalty [54].

15. References

[1].Allen, J. (2001). CERT System and Network Security Practices, in Proceedings of Fifth National Colloquium for Information and communications systems Security Education, George Mason University, Fairfax, Virginia, 22-24 May. Retrieved 23 Novemer 2017, from http://www.theebusinesssite.com/PPT/SecureWebsites-769468/769498_Reading_Class8-CERT_Network_Hardening.pdf

[2].American Society for Industrial Security (ASIS). (2004). Cybercrime-Fighting Tools Still Lacking, Security Management, number 40.

[3].Anderson, R. (2001). Why Information Security Is Hard--an Economic Perspective, in Proceedings of the 17th Annual Computer Security Applications Conference, Washington, DC: IEEE Computer Society. Retrieved 23 Novemer 2017, from http://www.acsac.org/2001/papers/110.pdf

[4].Behar, R. (1997). Who's Reading Your E-mail? Fortune, number 66, pp. 57-70.

[5].Bequai, A. (1978). Computer Crime, Lexington, Massachusetts, Toronto: Lexington Books.

[6].Carter, D. L. (1995). Computer Crime Categories, Law Enforcement Bulletin, U. S. Department of Justice: Federal Bureau of Investigation, volume 64, number 7, pp. 21-26.

[7].CCIPS. (2006). Computer Intrusion Cases. Retrieved 23 Novemer 2017, from http://www.usdoj.gov/criminal/cybercrime/cccases.html

[8].Centre for Strategic and International Studies (CSIS). (1998). Cybercrime Cyberterrorism Cyberwarfare: Averting an Electronic Waterloo (CSIS Task Force Report), Centre for Strategic and International Studies.

[9].Clark, F. and Diliberto, K. (1996). Investigating Computer Crime, Boca Raton, Florida: CRC Press LLC.

[10]. Collin, B. C. (1999). The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge, 11th Annual International Symposium Criminal Justice Issues. Retrieved 23 Novemer 2017, from http://www.crime-research.org/library/Cyberter.htm

[11]. Conly, Catherine H. (1991). Organizing for Computer Crime Investigation and Prosecution, Darby, PA: Diane Publishing.

[12]. Cook, D. (1997). Poverty, Crime and Punishment, London: CPAG.

[13]. CSI. (2000). CSI/FBI 2000 Computer Crime and Security Survey.

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

[15]. Daler, T., Gulbrandsen, R., Melgrd, B. and Sjølstad, T. (1989). Security of Information and Data, Chichester: Ellis Horwood.

[16]. Davidson, A. (14 April 2003). Decentralization, Disease and Terrorism. Retrieved 23 Novemer 2017, from http://www.eclicktick.com/decentralization__disease_and_terrorism__.htm

[17]. Dnes, A. W. (2000). The Economics of Crime, in N. G. Fielding, A. Clarke and R. Witt. (eds.). The Economic Dimensions of Crime, London: Palgrave, 2000, pp. 70-81.

[18]. Dong, S. & Li, X. (2016). Besieged privacy in social networking services. International Journal of Electronic Security and Digital Forensics. Vol. 8, Issue 3. pp. 224-233. Retrieved 23 November 2017, from https://www.inderscienceonline.com/doi/pdf/10.1504/IJESDF.2016.077447. DOI: 10.1504/IJESDF.2016.077447

[19]. Feldman, P. (1993). The Psychology of Crime, New York, NY: Cambridge University Press.

[20]. Felson, M. (2002). Crime and Everyday Life, third edition, Thousand Oaks, California: SAGE Publications.

[21]. Fields, G. (6 April 2004). Cyberexperts and Engineers Wanted by FBI, Wall Street Journal, B1.

[22]. Gelbstein, E., and Kamal, A.(2002). Information Insecurity: A Survival Guide to the Uncharted Territories of Cyber-threats and Cyber-security, the United Nations Information and Communications Technology Task Force and the United Nations Institute for Training and Research.

[23]. 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 23 Novemer 2017, from http://www.aic.gov.au/conferences/transnational/grabosky.pdf

[24]. Gray, C. M. (1979). The Costs of Crime: Review and Overview, in C. M. Gray. (ed.). The Costs of Crime, Beverly Hills, CA: SAGE Publications, pp. 13-32.

[25]. Greenberg, M. S. and Ruback, R. B. (1985). A Model of Crime Victim Decision Making, Victimology: An International Journal, volume 10, pp. 600-616.

[26]. Hatcher, M. and co-workers. (1999). Computer Crimes, American Criminal Law Review, volume 36.

[27]. Hoo, J. S. (2000). How Much is Enough? A Risk Management Approach to Computer Security, Centre for International Security and Cooperation Working Paper. Retrieved 23 Novemer 2017, from http://iis-db.stanford.edu/pubs/11900/soohoo.pdf

[28]. Institute for Security Technology Studies (ISTS). (2002). Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Needs Assessment.

[29]. International Monetary Fund (IMF). (2002). Global Financial Stability Report, A Quarterly on Market Developments and Issues, International Monetary Fund.

[30]. Johnson, T. A. (2006). Forensic Computer Crime Investigation, Boca Raton, Florida: Taylor and Francis Group.

[31]. Kelly, J. X. (2002). Cybercrime - High Tech Crime, JISC Legal Information Service - University of Strathclyde. Retrieved 23 November 2017, from http://www.jisc.ac.uk/legal/index.cfm?name=lis_cybercrime

[32]. Kingdon, J. (1994). Shooting the Messenger: The Liability of Internet Service Providers for Prohibited Expression. Retrieved 23 Novemer 2017, from http://www.catalaw.com/logic/docs/jk-isps.htm

[33]. Lee, M. and co-workers. (1999). Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal, Berkeley Technological Law

Journal, volume 14, number 2, pp. 839-885.

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

[35]. Li, X. (2008a). The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited Through Typical Cases Prosecuted. University of Ottawa Law & Technology Journal, 5, 125−140.

[36]. Li, X. (2008b). Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society. (University of Turku). Turku, Finland: University of Turku.

[37]. Loeb, M. P. (1 April 2004). The True Cost of Cybercrime, Network Computing.

[38]. London School of Economics and Political Science. (2001). Cybercrime: the Challenge to Leviathan?. Retrieved 23 Novemer 2017, from http://www.lse.ac.uk/clubs/hayek/Essays/cybercrime.htm

[39]. Mandia, K. and Prosise, C. (2003). Incident Response and Computer Forensics, Emeryville, California: McGraw-Hill/Osborne.

[40]. McAfee. (2005). Virtual Criminology Report: North American Study into Organized Crime and the Internet.

[41]. McConnell International. (2000). Cyber Crime . . . and Punishment? Archaic Laws Threaten Global Information. Retrieved 23 Novemer 2017, from http://www.witsa.org/papers/McConnell-cybercrime.pdf.

[42]. McCullagh, D. (19 August 2004). Punishment Fails to Fit the Cybercrime, ZDNet United Kingdom. Retrieved 23 Novemer 2017, from http://www.crime-research.org/news/19.08.2004/574/

[43]. McKenna, B. (2003). United Kingdom Police Promise Charter to Guard Good Names, Computers and Security, volume 22, number 1, pp. 38-40.

[44]. Miethe, T. D. (1995). Fear and Withdrawal from Urban Life, in Wesley G. Skogan, ed. Reactions to Crime and Violence, Thousand Oaks, London, New Delhi: SAGE Periodicals Press, pp. 14-27.

[45]. Miettinen, J. E. (1996). Survey of Hacking in Finland in the 1990s- Summary of the Results, Oulu: University of Oulu.

[46]. Mitchell, C. (2012). The Cyber Crime Threat on Mobile Devices. Retrieved 23 Novemer 2017, from chrismitchell.net/Papers/tcctom.pdf

[47]. Mitchell, S. D., and Banker, E. A. (1998). Private Intrusion Response, Harvard Journal of Law and Technology, volume 11, number 3, pp. 699-732.

[48]. Mohay, G., Byron, C., Vel, O., McKemmish R., and Anderson, A. (2003). Computer and Intrusion Forensics, Norwood, Massachusetts: Artech House.

[49]. Molnar, J. (1987). Putting Computer-related Crime in Perspective, Journal of Policy Analysis and Management, volume 6, number 4, Privatization: Theory and Practice, pp. 714-716.

[50]. NPA. (1998). The Situation of High-tech Crime and the Suppression of Police, Japan Police White Paper, Tokyo: National Police Agency.

[51]. Nycum, S. H. (1983). Testimony on Computer Security before the U. S. Senate Subcommittee on Oversight of Government Management of the Committee on Governmental Affairs, Computers and Society, volume 13, number 4 and volume 14, Nos. 1, 2, and 3.

[52]. Pethia, R. D. (2001). Information Technology—Essential But Vulnerable: How Prepared Are We for Attacks? Before the House Committee on Government Reform,

[53]. Philip, A. R. (2002). The Legal System and Ethics in Information Security,

SANS Institute, 2002. Retrieved 23 Novemer 2017, from http://www.securitydocs.com/go/1604

[54]. Radzinowicz, L. and King, J. (1977). The Growth of Crime: The International Experience, London: Hamish Hamilton.

[55]. Roush, W. (1995). Hackers: Taking a Bite Out of Computer Crime, Technology Review.

[56]. Salgado, R. P. (2001). Working with Victims of Computer Network Hacks, USA Bulletin, volume 49, number 2.

[57]. Schneier, B. (2004). Hacking the Business Climate for Network Security, Computer, volume 37, number 4, pp. 87-89.

[58]. Sieber, U. (1998). Legal Aspects of Computer-Related Crime in the Information Society, The COMCRIME-Study for the European Commission. Retrieved 23 Novemer 2017, from http://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html

[59]. Sinrod, E. J., and Reilly, W. P. (2000). Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws, Computer and High Technology Law Journal, volume 16, pp. 177-232.

[60]. Smith, R. G., Grabosky, P. and Urbas, G. (2004). Cyber Criminals on Trial, Cambridge: The Press Syndicate of the University of Cambridge.

[61]. Sofaer, A. D. and Goodman, S. E. (eds.). (2001). The Transnational Dimension of Cyber Crime and Terrorism, Hoover Institution, pp. 35-68.

[62]. Speer, D. L. (2000). Redefining Borders: The Challenges of Cybercrime, Crime, Law and Social Change, volume 34, pp. 259-273.

[63]. Stanley, T. J. (1995). Optimal Penalties for Concealment of Crime, Economics Working Paper Archive.

[64]. Stephenson, P. (2000). Investigating Computer-Related Crime, Boca Raton: Florida: CRC Press LLC.

[65]. Stoll, C. (1988). Stalking the Wily Hacker, Communication of the ACM, volume 31, number 5, 484-497. Reprinted in C. Dunlop and R. Kling (eds.) Computerization and Controversy: Value Conflicts and Social Choices, San Diego: Academic Press, 1991, pp. 524-532.

[66]. Telang, R, and Wattel, S. (2005). Impact of Vulnerability Disclosure on Market Value of Software Vendors: An Empirical Analysis, Presented at the Fourth Workshop on Economics and Information Security, Boston, 1-3 June.

[67]. Thompson, D. (1989). Police Powers - Where's the Evidence? Proceedings of The Australian Computer Abuse Inaugural Conference.

[68]. Tullock, G. (1967). The Welfare Costs of Tariffs, Monopolies and Theft, Western Economic Journal, volume 5, pp. 224-232.

[69]. UNCJIN. (1999). International Review of Criminal Policy -United Nations Manual on the Prevention and Control of Computer-Related Crime, International Review of Criminal Policy, nos. 43 and 44.

[70]. Vacca, J. R. (2005). Computer Forensic: Computer Crime Scene Investigation, Hingham, Massachusetts: Charles River Media.

[71]. Vamosi, R. (10 September 2003). Make the Punishment Fit the Cybercrime, CNET Reviews. Retrieved 23 Novemer 2017, from http://reviews.cnet.com/4520-3513_7-5073597-1.html

[72]. Walsh, D. P. (1983). Visibility, in Dermot Walsh and Adrian Poole (eds), A Dictionary of Criminology, London, Boston, Melbourne and Henley: Routledge and Kegan Paul.

[73]. Wasik, M. (1991). Crime and the Computer, Oxford: Clarendon Press.