Received for publication: 19.2.2017.
UDK: 343

Review paper

A Review of Motivations of Illegal Cyber Activities

Xingan Li
School of Governance, Law and Society, Tallinn University, Estonia

Abstract

Illegal cyber activities have been developing in past three decades with the mounting number of users of the computer and mobile networks. Potential perpetrators obtained more opportunities to instigate cyber attacks at different targets, at different scales, and from different motives. The existence of motivated attackers is one of an underlying trinity (together with the potential victims and weak guardianship) that leads to illegal activities (Cohen and Felson, 1979). In order to deal with illegal cyber activities, it is indispensable to have a better understanding of motivations of those potential attackers. The purpose of this article is to explore into motivation behind sophisticated illegal cyber activities, with an emphasis on reviewing findings in law enforcement as well as previous scholarly research. It was found that the motives of illegal cyber activities might diverge significantly from one another, but they might also have enormous similarity in that they were frequently directed to grey areas of social lives.

Keywords: illegal cyber activities, criminal hacking, cybercrime, motivation, criminal psychology, social control

Introduction

Conventional manners of production, services, and life have been to some degree toppled by the developing information and communications technology (ICT) since mid-1900s. The quantities of PCs and Internet clients continue expanding; the numbers of web sites, Internet hosts, web pages and transmission capacity continue developing; and the size of web based business and e-administration continues growing (Li 2008, pp. 82-89). Cybersecurity can be understood as a relative concept: neither can consummate security be achievable, nor does absolute insecurity exist (Li 2006a; Li 2006b). Vulnerabilities of the information society undermine the likelihood of society's yearning to a positive scene (Li 2008, pp. 89-111). Cyberinsecurity and illegal cyber activities impose new work stack on people thinking about interests of this era. With the enlarging group of Internet clients and expanding extent of information-related actions, the potential culprit of illegal cyber activities acquire more chances to launch assaults of different scales and from different motives. The likelihood of relocating conventional illegal activities into cyberspace has alerted law enforcement to struggle against existing illegal cyber activities and to prepare for rising threats (Li 2008, p. 64).

The motivated illegal actor is one of a causal trinity (together with the potential victims and weak guardianship) that leads to offences (Cohen and Felson, 1979). In illegal cyber activities, this is also a perceivable reality. While the three factors are considered intertwined together, this article will be dedicated particularly to depicting factors motivating potential illegal cyber attackers. It is of special significance for both law enforcement and policy-makers to base their effort on an understanding of the internal power that pushes the potential perpetrators to commit illegal cyber activities. If motives behind an illegal cyber activity can be identified, it can help to explain how

such activity is committed, what forms of digital media are exploited, and how the detection can be preceded. Research in motives of illegal cyber activities can also help policy-makers to decide on what kind of countermeasures are more effective to discourage potential perpetrators from carrying out the activities.

After this introduction, the following section will be contributed to briefly review previous studies and research in classification of motives as of illegal cyber activities. The third section, based on both review of previous research and review of practical cases, will list different possible types of motives involved in the illegal cyber activities. It is neither designed nor possible to give an exhausted list. Distinction between some items can be very obvious, while that between some other items can be very slight. Therefore, it can be found that some of the items can even be combined as one. However, in this study, efforts are made to distinguish as many categories as possible, not vice versa. The final part will conclude the whole article and give some indications in applicable fields that such a research can be extended to.

Previous Research

The intentions of digital culprits could be exceptionally broad and cover many different sorts of offenses (Li 2008, p. 152). Although it is complex to unearth a motive under illegal cyber activities (Philip 2002, p. 7), abundant different studies and research have drawn wide-ranging conclusions on the classification of motives. Jordan and Taylor (1998) listed six common attitudes amongst hackers: addiction, curiosity, thrill of information searches, ability to access, peer recognition, and identifying security loopholes. Maiwald (2003, pp. 36-38) has concluded that hacker motivations had fell into three groups, including the quest for challenge, greed, and malicious intent or vandalism. Kiger and co-workers (2004) have summarized the motivations of illegal cyber activities as money, entertainment, ego, cause, entrance to social groups, and status. Pipkin (2002, pp. 17-28) has proposed that hackers might hack from a sense of intellectual motivation, such as educational experimentation, harmless fun, as a wake-up call; personally motivated, such as disgruntled employees, cyber-stalking; socially motivated, such as cyber-activism; politically motivated, such as cyber terrorism, cyber-warfare; financially motivated; and motivated by ego. Kremen (1998) has classified hackers into ten types with "different sizes, flavours and colours," including curious hacker, thrill seeker, the person who wants information about computers and their flaws, power seeker, vandal, the person who steals industrial information, secrets and/or intellectual property, the person who steals money, the person who performs industrial espionage, terrorist, and international spy (Li 2008, p. 152-153).

In fact, the motives of illegal cyber activities may differ in a manner that is outside the imagination. If we articulate that various perpetrators have similar motives, we can also articulate that virtually each perpetrator has his or her own. Bequai (1983, pp 44-45) has summarized 17 different kinds of motives that push the probable perpetrators to run the risk of committing illegal cyber activities (Li 2008, p. 153).

Illegal cyber activities affect several scientific disciplines (Li 2008, pp. 157-166). In studies on illegal cyber activities, the word motivation is used in a broad sense, and is habitually interchangeable with motive. Motives are nothing more of a mystery than the wants and wishes the

goal-directed activities attempt to satisfy (Smith 1998, p. 422). A stringent distinction cannot be made between these two words. The forces behind the individuals' decisions to perpetrate illegal cyber activities are dissimilar with each other.

Specialised Modes in Diversified Motives

This section will categorize and examine various kinds of the commonest motives based on review of literature and cases. Of course, it is not designed to provide an exhausted list of all motives, but is looking into details of the complicacy of the psychological aspect of illegal cyber activities.

1. Pursuing free flow of information

A free flow of information is a requirement for ensuring the free movement of goods, persons, services and capital (Directive 95/46/EC, Preamble (3)). In cyberspace, people who hold the view that the Internet is a public place, and thus everyone has the right of obtaining information, are not rare. Under the dominance of the hypothesis of information freedom, many information systems users take the risk of breaching others users' privacy and trade secrets. Levy (1984), Selwyn and Gorad (2001), and Himanen (2001) have shown that many traditional hackers are motivated by a belief in the freedom of information. These hackers have insisted that all the useful information must be freely copied, distribute, studied, changed, and improved, but their ethical code prohibits destructive activities against any information (See Branscomb 1990). The focus of the hacker ethic is on the freedom of information. The hacker ethic was initially created by the MIT hackers in the late 1950s to the late 1960s and articulated by Steven Levy in his book "Hackers: Heroes of the Computer Revolution." The general creed includes the following aspects: "1. Always yield the Hands-On Imperative! Access to computers-- and anything else which might teach you about the way the world works-- should be unlimited and total. 2. All information should be free. 3. Mistrust Authority-- Promote Decentralization. 4. Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position. 5. You can create art and beauty on a computer. 6. Computers can change your life for the better." (See Logik Bomb, Hacker's Encyclopedia, Second Revised Edition, 1997). What is problematic is that unauthorized access to confidential data has been criminalized, even in pre-computer times. If e-mail is comparable to a letter, and if free information advocators can freely open e-mail, a natural conclusion will be that everyone can destroy mailboxes and open letters. The only difference is that the present files exist in digital form. Access to confidential information is punished by laws penalizing offences infringing privacy, intellectual property, trade secret, and state secret. Therefore, the freedom of information is limited to information that is granted free access but access is not free to information that is limited. The other end of the free flow of information is the safeguard of the fundamental rights of individuals (Directive 95/46/EC, Preamble (3)).

2. Realizing free expression of ego

Hackers also have the possibility of hacking for the sake of their ego, for proving a self that is different from the selves of others. Perpetrators in this category are usually frustrated in social competition elsewhere and seek an opportunity to compensate by employing their computer

techniques. Through success in surrendering to information systems, they supersede others in hacking techniques and skills, even though they have an apparent inability that leave them incompetent with others in social activities generally. Yan and Zhang (Beijing Youth Daily, 6 November 2001) have reported the case where a 17-year-old hacker intruded into an official human-resources web site, defaced the homepage, formatted the hard disk of the server, and destroyed a great deal of data. It was reported that during his sick leave at home, the hacker had picked up his hacking knowledge from the hackers' web sites, and downloaded some hacking programmes. Then he found some web sites with security holes and intruded into them. At first, he sent messages to the administrators of these web sites, telling them that their web sites had loopholes. Without receiving any reply, he got angry and defaced some of these web sites (Yan and Zhang 2001).

3. Taking technical challenge

Technical challenge has been long identified as a motivation. Pipkin (2002) regarded challenge as the biggest motivation, meaning that the hacker is excited after succeeding in his attack on most secure systems. In one case, a hacker created a Trojan programme named IPXSRV, and gained control of 60,000 computers. He created a botnet, that was "a collection of compromised computers controlled by the same intruder, often [using] remote control software or Internet Relay Chat (IRC) services" (Daintith 2004, p. 56). The hacker manoeuvred this colossal "botnet" to launch denial of service attack against a music web site for three months before the police detected it. Investigation revealed that the hacker had been seeking a chance to try the power of his Trojan programme, and chose this web site as a target of denial of service attack. As a result, the web site was broken down for three months (Secretchina 17 March 2005).

4. Curiosity of seeking new knowledge

Illegal cyber activities, motivated by a desire to seek knowledge, are not rare in practice. Jordan and Taylor (1998) reported the motivation of Kevin Mitnick, the most famous of all hackers was to gain knowledge, seeking a better understanding of information systems.

Many computer and Internet users are motivated to acquire knowledge from the devices, information and new space. Both hardware and software are the targets of their knowledge-seeking attempts. Hackers are seeking knowledge through access to others' computers by fair means or foul. "The Hacker Manifesto" clearly expressed the motivation behind hackers of this kind. It stated that cyberspace was a world of "the electron and the switch," and hackers were called criminals due to their use of the services without paying during their seeking after knowledge motivated by curiosity (The Mentor, The Hacker Manifesto, 8 January 1986).

5. Testing system security and resilience

Technical primacy is one of the most important answers to the question "what do hackers hack for?" The common sense knowledge about the attacks is that hackers identify flaws in systems or software, to allow the developers or the administrators to fix them (See Branscomb 1990, p. 24). For example, Brian West used MS Front Page and a web browser to identify a security flaw in some web sites that allowed him to have access to proprietary information and password files

(See U. S. Department of Justice, Press Release, 24 September 2001). Hacking for security may be quite the same to hacking for insecurity: on the one hand, the unauthorized intrusions into the protected systems are illegal; on the other hand, the publication of security flaws also poses a real danger for the systems.

In addition, some physical damage to information systems is also possible when testing the resilience of factors under operating conditions. For example, in R. v. Feltis ([1996] EWCA Crim 776 (19th August, 1996)), one of the explanations of the accused about why he had apparently sabotaged the company's computer was that he had been testing the computer, and particularly its resilience to interference, by disconnecting two cables and reconnecting them, as a result of which an impairment of the computer was caused and an enormous disruption of the business of the company occurred.

6. Taking adventure in cyberspace

Traditional adventurers have sought psychic satisfaction from conquering things others have seemed unable to do, and during which they overcame unimaginable difficulties. The modern adventurers have also found challenges in the field of technology, from telecommunications, computers to the networks. The ability to influence huge systems may be satisfying in and of itself (See Ministry of Justice 1985, p. 206; Howerton 1985, p. 54; the United Nations Crime and Justice Information Network 1999, Paragraph 74; Schwartau 1994; Branscomb 1990, p. 24; Grabosky 2000). Creator of Melissa Computer Virus said that he had constructed the virus to evade anti-virus software and to infect computers using the Windows 95, Windows 98 and Windows NT operating systems and the Microsoft Word 97 and Word 2000 word processing programmes (See United States v. Smith (D. NJ) 2 May 2002). Activities, either benign or malicious, on the "electronic frontier" involve the factor of adventure, that is to say, to explore the unknown (Grabosky 2000, pp. 2-3). What Donn B. Parker called the personification of computers (Parker 1998) is also such a motive. Sophisticated viruses indicate that writers who believe that their works contribute to the development of science and technology have created them (Kabay 2001).

Adventure is closely associated with the conception of curiosity. Under the drive of curiosity, considerable examples of such curious intrusions have happened, which had catastrophic effects (Howerton 1985, p. 54).

Adventure is not always a simple motive that can be explicitly identified. Sometimes, it is closely related to other motives, and in other cases, the adventure motive may be ambiguous. According to The Associate Press (19 March 1998), when the hacker, who called himself "The Analyser", and launched an attack against the Pentagon's computer systems, was identified by the U. S. Department of Justice and questioned by a special police anti-hacker unit, the chief administrator of the country from where the 18-year-old boy came praised him: "Damn good, very dangerous, too" (Pentagon hacker Wins Praise, Associated Press, 19 March 1998). Soon after the incident, the hacker was drafted into the national army to serve in an information warfare division, an assignment which utilized his computer talents (Israeli Teen Hacker Details Prowess, Associated Press, April 1998).

7. Practising and show up programming skills

In contrast to testing hackers who try to identify flaws in computer systems, experimental hackers try to reveal the functions of hacking programmes. Whether the systems are secure or not is irrelevant. Actual intrusion into the systems is only an occasional result. Many Internet users did experiments of this kind with software downloaded from the Internet, or programmes compiled by them, and sometimes no actual intrusion succeeded. Relatively unprepared and unintended, experimental hackers are usually the "first offender". Their purpose is to test the function of intrusion programmes or techniques, during which they accidentally succeed in acquiring unauthorized access to the systems.

8. Tentative attacks against potentially vulnerable devices

Tentative hackers are similar to experimental hackers in the way that they are unprepared intentional intruders. Nevertheless, a distinctive point is that tentative hackers try to use hacking programmes or intrusion techniques. Whether the system is secure and whether the intrusion is successful are both irrelevant considerations. For example, some users operate password-cracking programmes to access others' encrypted information. Internet users sometimes also try to guess other users' account ID and passwords so as to enter their systems.

9. Hacking out of hatred

Hatred may come into being for a variety of reasons. Dissatisfied employees damage their employers' assets. Dissidents are motivated to destroy the states' critical infrastructure. The hacktivists, anarchists, and terrorists all launch attacks against targets regardless of their nature. Generally, hatred leads to attempt to weaken the counterparts' social priorities. Examples include ruining computer systems (For example, in prosecuted cases such as United States v. Garcia (C. D. Cal.) 23 February 2004; United States v. Diaz (S. D. Fla.) 5 December 2003; United States v. Patterson (W. D. Pa.) 2 December 2003; United State v. Lloyd (D. JN) 26 February 2002; United States v. Ventimiglia (M. D. FL) 20 March 2001; United States v. Sullivan (W. D. NC) 13 April 2001; United States v. McKenna (D. NH) 18 June 2001); destroying information (Howerton 1985, p. 55); revealing confidential data (Grabosky 2000, pp. 2-3); and defacing abhorrent web pages (Grabosky 2000, pp. 2.-3).

Envy may also lead to hatred. In illegal cyber activities, attackers commit sabotage due to envy of others' wealth, competitors' success, and colleagues' achievements.

10. Hacking for acquiring financial gains or avoiding payment

Not only has information itself value, but information systems are also used widely in the financial sector (Parker 1998). Because the function of the computer in accounting enables a wide use of computers in financial management, embezzlement has been made easier by numerous methods (Howerton 1985, p. 54). These methods may include information selling without the right to do so; extorting from the victimized organization; embezzling from employers; illegally obtaining information to sell to competitors; electronic theft of credit-card numbers; and stealing personal information to impersonate someone financially (Ministry of Justice 1985, p. 206).

The perpetrators steal, swindle, embezzle, and blackmail property in order to maintain a livelihood, seeking ease and comfort, repaying gambling debts (Parker 1998), or avoid payment. In Morgans v. Director of Public Prosecutions ([2000] UKHL 9; [2000] 2 All ER 522; [2000] 2 WLR 386; [2000] Crim LR 576 (17th February, 2000). The conviction was overruled due to the matter of obtaining the evidence, which was obtained through the installation of an interception device into the telephone line of the accused), the accused used the telephone line to acquire unauthorized access to the computer systems of several different companies, thus obtaining telecommunication services without payment. In the face of deliberate financial hackers, even the most secure systems on the Internet are meeting universal threats.

In fact, financial hacking is not always as sophisticated as imagined by the public, for sometimes hackers may be the software provider. This is a serious threat for the banking system.

11. Resulting illegal activities due to educational reasons

This kind of hacking is the unauthorized use of the systems for educational purposes. In the early stage when computer hardware, software, and network services were expensive, they could only be obtained by a limited number of big organizations and universities. Many hackers tried to use the system for educational purposes without permission. Nevertheless, with the development of less-bulky, low-cost personal computers, this kind of educational hacking has become history.

12. Hacking to change academic results

University students hack for better scores or grades in academic records. In August 1977, officials at a large university in the U. S. uncovered a scheme involving payments by students who wanted their grades altered in the school's computer centre. Investigators found that several thousand dollars had been paid to a university employee who made changes on grade cards that were later used to make entries in the university's computer (Lehigh University Uncovers Payment to Alter Grade of Student, New York Times, 1 September, 1977, A-18). From then on, dozens of students in the U. S. have been caught hacking into school computers to give themselves better grades. In one case, nineteen students were suspended after being accused of knowingly involved in electronically changing their transcripts. Seven other students were told their grades were altered. Nevertheless, this was apparently done without their knowledge (Anderson 2002).

13. Motivation for harassment and murder

Internet harassment can occur in nearly every Internet service to direct obscenities toward others, and make insulting statements based on gender, race, religion, nationality, or sexual orientation (Kelly 2002). In offences where information systems are used as means of committing verbal assault, threat, harassment, alarming, spam and fraud, the motivation of the perpetrator is to harass and to kill the victim. The function of the Internet as a means of communications and with a high anonymity of interaction often entraps the victims into unforeseeable dangers. In 2005, China Ministry of Public Security investigated 1,000 assassination cases, in many of which the potential illegal attackers found the potential victims through the Internet (Yi 2006). In many cases of illegal

cyber activities, stalkers and murderers find and entice victims through the communication and interaction of various Internet services.

14. Mobilizing political movement

For many years, defence forces, governments, and even computer companies have been popular targets for sabotage attacks. According to Daler and co-workers (1982), political groups in France repeatedly damaged computers, asserting that computers were the favoured tools of those who dominate. Italy, the former West Germany, the U. S., the U. K., Japan, and the Scandinavian countries have experienced sabotage as well, with both the old- and new-fashioned attacks on malicious programmes (Daler and co-workers 1982, pp. 24-25).

Political hacking also formed an extreme movement: "hacktivism". Hacktivists launch politically motivated attacks on public web pages or e-mail servers (Vatis 2000). In 1999, for example, the homepages for the White House was attacked by political activists protesting against the site's politics (See U. S. Department of Justice, Congressional Testimony on Cybercrime Strategy, 28 July 2000).

15. Launching cyber warfare

People worry that the threat of cyberwarfare will be a future nightmare because hacking communities have the ability to launch destructive attacks on computer systems. In recent years, a cyberwar was nearly taking place. In 1990, a hacker organization "Legion of the Underground" declared war on some countries in retaliation for human-rights violations. Several other hacker groups condemned the aggressive act, and soon after, the Legion of the Underground retracted their declaration of cyber war (For the story, see Palczewski 2001. For the joint statement, see 2600 and co-workers. Joint Statement Condemning LoU Cyberwar, *2600 News, 7 January 1999)*. Cyberwafare also happened in the initial years of the twenty-first century. Hacker groups became popular in East Asian countries during several cyber wars, mostly between hacker groups of different countries due to their positional differences on some international affairs. At that time, the relevant countries were highly vigilant to potential abuse of computers and networks and invested more heavily on information security control.

16. Unleash anti-computerization actions

As some people are against mechanicalization, electronization, industrialization, modernization, and globalization, others are against the process of computerization, informationization and networking. According to Parker (1998), some hacker sympathizers describe attacks as justifiable protests or direct action against enemies of the environment or of society in general.

Unabomber represented another kind of anti-computer "hacking". He carried out 16 bombings, which, altogether, killed three and injured 23 people (The offences were carried out during 1978 and 1995. As of 2004, Kaczynski was serving a life sentence without the possibility of parole in a maximum-security prison in Florence, Colorado). His "Unabomber Manifesto" claimed that technological progress brought about undesirable requirements for the people, and that the

people could stop this situation so as to recover their happier and simpler life close to nature (See Kaczynski 1996). Some other activists all over the world also destroyed a number of computers to protest against a computer society in which they thought that computers were being used to control people (The French activist group called CLODO, Comité de Libération ou de Détournement des Ordinateurs, committed the offence between 1979 and 1983). Indeed, they were not hackers in cyberspace, but traditional style bombers in real society.

17. Cyber Robin Hoods

Orthodox hackers hack in order to make programmes or information available to others free. As a hacker, Maelstrom, stated in an interview that he had never any feeling of moral apprehensiveness when he made Internet access accounts available to the public for free through hacking (Jordan and Taylor 1998, pp. 768-769).

Whether some charitable concerns or individuals will also crowd online to hack for money is an unanswered question. A hacker initially wanted to test how the security level of the mobile communications networks. After he found that he could make money through selling the cards with revised passwords, he opened a specific bank account in which to deposit the money, a separate account from his own daily-used bank account. He said that he did not hack for himself, but for the wellbeing of others. He donated 200 Renminbi Yuan (about 20 euros) to a leukaemia patient (Gao 2006).

Cyber Robin Hoods do not always publicize their intent. But on some web sites, methods for counterfeiting money are published.

18. Motivated by unfair competition

In order to enhance competitive capacity, businesses also engage in attacks against competitive rivals. In the 1990s, when the Internet economy boomed, many big online enterprises secretly attacked the web sites or defame the reputation with each other. Attackers benefit from the decline of competitors and from the increase in their own market share. They even practice access to each other's computer systems to obtain business secrets. In the rapid development of the information market, such destructive or espionage activities are fatal to the victimized enterprises.

19. Executing trap marketing

Some anti-virus compilers plant computer viruses and other destructive programmes into their anti-virus software to force users to purchase the upgraded versions of anti-virus software they compile or sell. By doing so, they hope to increase the market share and sale of their own products (Jiang and Yu 1997, pp. 18-27). Web sites owners also frequently use this trap marketing. Cookies are an example that is widely known and accepted. In malicious marketing cases, some web sites infect users' computers with embedded harmful codes and instruct the users of infected computers to visit their web sites repeatedly and to pay for cleaning the computer. Other forms of entrapment also include kidnapping computers or programmes in order to render the machine repeatedly operating in a way benefiting code writers or spreaders. Web browser manipulation is

one such abduction that controls the homepage, or even the whole browser, and is directed solely to the perpetrators' web sites.

20. Motivated by self-defence

Hacking has also been used for self-defence. For example, in order to prevent illegal replication of software, a pair of Pakistani bothers bundled "Brain Virus" into their software and attacked Delaware University in October 1987 (Forester and Morrison 1994, p. 93). Their idea was that only those who pirated the software would be victimized, the virus being an automatic retributive tool. The followers of a religious cult in an Asian country also attacked the satellite communications systems as a means of self-defence. The government charged the religion with being an "evil cult" and prohibited its practice. In revenge, members of this forbidden religion used the Internet to hack several times into the satellite broadcasting system, and changed the official TV programmes to video programmes disseminating the "truth" about this religion.

The idea of the above-mentioned "Pakistan virus" is not without descendants. Many trial versions of software (or shareware) include similar idea in expressive form. While some of the trial versions can work in one way or another after the trial period, other trial versions can be completely disabled. For example, a certain kind of operating system provides a 30-day trial period, after which the system cannot be operated without registration, which implies a process of purchasing. Without the operating system, the computer is simply broken down --analogous to an attack launched by a logic bomb, except that it is an "attack" under the cover of failure to register after the trial period.

21. Hacking for recreation

Both recreation and hacking are exciting. Randall and co-workers (2000) found that excitement was a major reason for hacking. Here, hacking has an equivalent function to entertainment. Although computing is different from gaming, the computer has a close relationship with gaming. Not only are computer and online games prevalent, but the use of the computer and the surfing of the Internet may serve gaming instinct. Many users enjoy online surfing, interaction and self-publishing, but fewer experience success in accessing and controlling others' information. But by overcoming the slight difficulty in cracking users' password or other access-control measure, a unique pleasure is afforded to users who experience this victory.

22. Employment-related motivations

Although considerable hacker activities are in fact illegal, the successful hacker will usually be admired for his or her skills. At the same time, many hackers have been offered a well-paid job as a computer expert or even security manager. For example, Robert T. Morris, was one such. He created the Morris Worm in 1988, infecting about 6,000 computers and causing losses that ranged from 200 to 53,000 dollars each. At present, on his web site, he writes that: "I'm at the MIT Computer Science and Artificial Intelligence Laboratory…" (Retrieved 10 January 2017, from *http://pdos.csail.mit.edu/~rtm/*)

Banks (1997) related hacking to employment, which means that if the hacked system owners caught the hacker, they would employ the hacker exactly to protect the systems from other intruders.

A high-profile employer can employ a hacker who has damaged thousands of computers and caused losses of millions of dollars, a natural analogy is that a better chance of employment should be hacked together through millions of computers, and billions of dollars of losses. Alternatively, less skilful hackers might try to damage some hundreds of computers and obtain an ordinary job offer. Illegal hackers are usually better off after their hacking activities have been made public.

By saying this, we are not making complaint about a function of the judicial system that allows the rehabilitation of those who have committed offences in this way. In contrast to the ideal "general deterrence," the question arises as to whether such a practice serves a generally-motivating role.

Employment-related hacking is not limited to getting employment opportunities through hacking. Hackers have sometimes hacked as a form of retribution when an employer has not provided an offer. Skeeve Stevens seriously damaged the AUSNET, an Internet company that refused to employ him. He had compromised 1,225 credit cards and displayed a message on the company's homepage in April 1995, saying, "AUSNET is a disgusting network … and should be shut down and sued by all their users!" (Phrack Magazine, volume 8, number 53, 8 July 1998, article 14 of 15, 0Xd) In addition, in DPP v. Lennon (Director of Public Prosecutions v Lennon [2006] EWHC 1201 (Admin) (11 May 2006)), after being dismissed, the accused had downloaded a mail-bombing programme from the Internet and used it to automatically send about 5 million e-mails to the former employer's e-mail servers. His purpose was to bring in the company into a "mess" and did not think his action was illegal.

23. Hacking for the hacker community

For those who regard themselves as hackers, "hacker" is a symbol, a label, a banner, a movement, a front, and a centripetal force, regardless of the fact that each hacker, particularly each of the malicious hackers behaves in a pattern that is not necessarily the same. Therefore, the hacker community is in reality a symbolic clan in which members "hack" in variant ways and for different ends.

Regardless of the fact that the members of the hacker community are heterogeneous, cases where hackers have united to take actions against legal or administrative measures targeted at certain "members" of their "hacker community" are not rare. The mere name of "hacker" may serve to raise an emotive force capable of bringing all kinds of hackers together, including traditional hackers, and hackers who are regarded as illegal cyber actors. In fact, in such a case, their activities are unreasoning: on the one hand, the activists do not belong to a single group; on the other hand, their targets are far from being only the web sites of the law-enforcement agencies. Their good will is to maintain the image of a "hacker community" as a whole, to prove their power against traditional government and law enforcement, and to resist an outside invasion.

Sub-culture was a term first used by A. K. Cohen in *Delinquent Boys: the Culture of the Gang* (1955) to denote a group or groups inside the host culture with different values from it, as evinced through their expression in deviant behaviour (Walsh 1983, p. 214). Zheng (2004) attribute this

motive to impact of the internal communications of the cyber attacker sub-cultural group. As to the situation in traditional illegal sub-cultural groups, these communications produce coherence inside the group. However, the network exists as a means of communications and enhances the communicative pattern of illegal cyber activities. Intrusion techniques and skills are the just contact-nodes for their members.

24. Destroying evidence contained in information systems

Information systems usually contain evidence for various kinds of cases, civil, criminal or administrative. The party for whom the evidence is unfavourable has a motive to destroy it, before or during the search and seizure by law-enforcement agencies. In R. v. Anitta Debnath ([2005] EWCA Crim 3472, No. 200501008A7), after the police began to investigate her harassment of the victim, the perpetrator paid a group of computer hackers to assist her to hijack the victim's e-mail, in order that the victim could no longer access the account.

25. Sexually motivated misuse

Sex exploitations cover a broad category of deviance. The most frequently prosecuted forms of sexually motivated misuse of information systems are the recording, depositing, transmitting, and trading of child pornography (See for example, United States v. Ziegler, No. 05-30177 D. C. No. CR-03-00008-RFC ORDER AND OPINION, 6 March 2007). In such cases, the perpetrator used the company's computer to view, deposit and exchange child pornography); sexual harassment through communication by using information systems; and promotion of illegal prostitution with the assistance of information systems.

Children are a particularly vulnerable group of people in society. Although international consensus has been achieved and treaties have been implemented requiring governments to "take all appropriate…measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse…" (UN Convention on the Rights of the Child, adopted and opened for signature, ratification and accession by General Assembly resolution 44/25 of 20 November 1989, entry into force 2 September 1990, Article 19), incidents, in which children are abused frequently happen. The abusers are increasingly using information systems to lure children to engage in sexual activity and spread child pornography. For example, in R. v. Kasam (2004 ONCJ 136 (CanLII), Docket: 10018867), the accused used his computer to collect hundreds of images and several video clips of child pornography (paragraph 2.5). In one compact disc were found 3,200 images of child pornography downloaded from the Internet (paragraph 2.4).

Besides sexual motives, there may also be present violent abuse of the child. These two aspects are closely connected with each other. In R. v. Sharpe, the court held that "the possession of child pornography and associated harms to children is the use of child pornography by paedophiles to groom children into committing sexual acts" (paragraph 205).

26. Anti-deviance

In both cases of United States v. Jarrett (Fourth Circuit No. 02-4953, 3 June 2003) and United States v. Steiger (Eleventh Circuit No. 01-15788, 01-16100 and 01-16269, 14 January 2003), hackers reported the cases and provided critical evidence for the law-enforcement agencies. They have never appeared before the court or been prosecuted. In other cases, such hackers were sued. In a civil case, Fischer v. Mt. Olive Lutheran Church (Western District of Wisconsin No. 01-C-0158-C, 28 March 2002), other employees in the Church suspected Fischer, a Lutheran minister, of engaging in sexual misconduct. They hired a computer expert to guess the password of the Hotmail account that the minister was known to use frequently. As a result, they cracked the password, looked through and printed the minister's messages, in some of which were included contents about sexual activity between the minister and other men (ibid.).

27. Comprehensive motives

In some other cases, the offenders have multiple motives, interrelated or unrelated with each other. For example, in R. v. Geller (2003 CanLII 31190 (ON S.C.), Docket: 493), the offender possessed 101 pornographic images, chatted with young girls of 13 or 14 years old in order to establish relationships (paragraph 5), obtained 400 credit cards and other personal information through hacking, accessed the Internet for 28 times without paying (paragraph 6), and engaged in activities that lead information systems to malfunction (paragraph 7).

28. Unclear motive

While many perpetrators act in a way to achieve something or destroy something, others act without reasonable reasons. In some cases, it is impossible to detect an impressive motive from the facts of the offence: the revelation of the abuse of information systems cannot lead to a clue for a useful identification of the state of mind. In State v. Moning, the accused used the computer terminal to obtain access to the database to run a query on the previous drug conviction of his acquaintance. After he printed a copy of the information, he handed the victim the printout. At this point, the victim became aware of the perpetrator's behaviour and reported his unauthorized access (2002-Ohio-5097).

29. (Not motivated but) influenced by psychological depression

In R. v. Taylor ([1998] EWCA Crim 1545 (12th May, 1998)), the accused woman illegally accessed the account of a man through computer systems and issued an unauthorized passbook for the account, with which an unidentified man attempted to withdraw £25,000, succeeded in getting £500 in cash but failed to get £24,500 in cheques. The opinion of the doctors showed that the woman was diagnosed as HIV positive during her committing the offence and was in a state of "clinical depression" which affected her judgment about her behaviour and the likely result of her behaviour.

If we pose the question as "what are all these listed motives in common," we can only answer it with a keyword: curiosity. Curiosity is an irresistible mental power, propelling people to know

the unknown and to control the uncontrollable, or to destruct the constructed, and to disorganize the organized, whether in the macro or the micro dimensions. Information systems are a dimension which has developed partly under the dynamics of human curiosity and has been threatened partly by this force.

Apart from the abundant findings identifying motives in this study, I found that for many hackers, instead of hacking for something, they have succeeded in hacking and then found something to obtain or destruct. The initial hacking was merely a random activity that accidentally succeeded in furthering additional actions. Successful hacking, it could be imagined, might lead to any kind of sabotage, destruction or vandalism, the obtaining of confidential or proprietary information, acquiring control over a system, and so on. Therefore, we can safely conclude that there are hackers who hack out of specific motives, and that there are also hackers who firstly hack and then find opportunities to reach specific goals. For hackers with specific purposes, the hacking process may be a sophisticated endeavour before they take hold of the compromised system, because they have to conquer the unknown continent of security. For hackers with less clear initial purposes without wanting to obtain something specific or destroy something specific, the hacking process may be more straightforward until the system is exploited, because they only harvest from a conquered land. These different hacking models imply that the goals can emerge before the beginning of the initial hacking or after the success of the initial hacking—in the latter case, the attempted hackers are likely to defend themselves by expressing the benign motive of wanting to face a technological challenge or a security loophole rather than by stating a malicious intent of economic espionage or sabotage. In this latter case, the motivation is that of a challenging adventure into the partially unknown.

Conclusion

Information systems store rich and colourful resources, attracting digital community constructors, conquerors, conspirators and criminals. With one-sixth of the population connected online, with a prolonged online time, and diversified online activities, it is natural that illegal cyber actors constitute a greater ratio among the Internet users, and that illegal cyber activities will constitute a greater proportion of overall illegal activities. If the unbalanced demographic distribution of computer and Internet users exists within different age groups, the comparison of their online behaviour is a valuable indicator in finding the reasons for this. The key concern in this comparison is that of the role of juveniles and young adults. Empirical studies have disclosed that youths may have more chances to use computers and the Internet and are more likely to commit illegal cyber activities and be victimized. The natural and social properties of different age groups have been shaped in different ways. Different have been their educational background, financial status, sense of responsibility, family structure, social interactions and interconnections, self-control, psychological make-up, and interest, knowledge, and skills. These distinctive characteristics determine that they are confronted with different chances and challenges in information systems, and in respect of gaining and losses in the online activities. As a result, young people are more likely to be involved in online adventures, stalking or stalked, exploiting or exploited, hacking or hacked.

The internal reasons why illegal actors are devoted to illegal cyber activities are connected with the functioning of information systems. This shows that the novelty and mobility of information systems enable people from quite different contexts to find something useful, valuable and profitable. Psychological satisfaction, spiritual enjoyment, financial obtaining, winning fame, opportunity getting, and fortune seeking are all realizable through the use and misuse of information systems. The motivations of committing illegal cyber activities are diversified. This means that illegal cyber activities are profitable for whatever purposes the attackers are pursuing. It makes sense that in cases motivated differently, the perpetrators may use different methods and thus leave different traces in the activities. Subsequently, this can help law enforcement to take actions to seize evidence of different forms.

To summarize, the illegal cyber actors may be satisfied in part by her or his having committed an illegal activity against the person and in part by his having committed an illegal activity against property. And there may be motives that can be met outside both these opportunities. Motives of likely offenders are different but barely novel (Grabosky 2000, pp. 2-3). The motives of illegal cyber activities might greatly vary from each other, but they might also have great similarity in that they were usually directed to grey areas of social lives. This explains why the hackers come out only "in the dark". In a broader perspective, studies of motives for illegal cyber activities will be useful for making feasible penal policy to eliminate the soil for such potentialities and to increase difficulty for such activities to be carried out. Such an interactive process between academic research and decision-making may enhances the prevention of deviance in the cyberspace.

References

Anderson, C. 2002. Hacking the Grade, Originally Aired, 3 September 2002. Retrieved 10 January 2017, from *http://www.techtv.com/cybercrime/internetfraud/story/0,23008,3396685,00.htm*

Banks, M. A. 1997. Web Psychos, Stalkers, and Pranksters: How to Protect Yourself Online, Arizona (USA): The Coriolis Group.

Bequai, A. 1983. How to Prevent Computer Crime: A Guide for Managers. New York, Chicago, Brisbane, Toronto, Singapore: John Wiley and Sons.

Branscomb, R. 1990. Computer Program and Computer Rogues: Tailoring the Punishment to Fit the Crime, Rutgers Computer and Technology Law Journal, volume 16, pp. 1-61.

Cohen, L. E., and Felson, M. 1979. Social Change and Crime Rate: A Routine Activity Approach, American Sociological Review, vol. 44, pp. 588-608.

Daintith, J. (eds.). 2004. Oxford Dictionary of Computing, fifth edition, Oxford: Oxford University Press.

Daler, T., Gulbrandsen, R., Melgrd, B. and Sjølstad, T. 1982. Security of Information and Data, Chichester: Ellis Horwood.

Forester, T. and Morrison, P. 1994. Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing, second ed., London: MIT Press.

Gao, Z. 2006. Hacker Tried for Theft of 3.7 Million from Beijing Mobile. Retrieved 10 January 2017, from *http://www.chinacourt.org/public/detail.php?id=196319*

Grabosky, P. 2000. Cyber Crime and Information Warfare, The Transnational Crime Conference convened by the Australian Institute of Criminology in association with the Australi-

an Federal Police and Australian Customs Service and held in Canberra, 9-10 March. Retrieved 10 January 2017, from http://www.aic.gov.au/conferences/transnational/grabosky.pdf

Himanen, P. 2001. The Hacker Ethic and the Spirit of Information Age, Great Britain: Secker and Warburg.

Howerton, P. W. 1985. Computer Crime: A Tutorial, ACM.

Jiang, H. and Yu, Z. 1997. Concerning Offence of Creating and Spreading Destructive Computer Program, Jurists, number 5, pp. 18-27.

Jordan, T. and Taylor, P. A. 1998. Sociology of Hackers, Sociological Review, volume 46 number 4, pp. 757-81.

Kabay, M. E. 2001. Studies and Surveys of Computer Crime. Retrieved 10 January 2017, from http://www2.norwich.edu/mkabay/methodology/crime_studies.htm

Kaczynski, T. 1995. The Unabomber's Manifesto: Industrial Society and Its Future, Jolly Roger. Retrieved 10 January 2017, from http://en.wikisource.org/wiki/Industrial_Society_and_Its_Future

Kelly, J. X. 2002. Cybercrime - High Tech Crime, JISC Legal Information Service - University of Strathclyde. Retrieved 10 January 2017, from http://www.jisc.ac.uk/legal/index.cfm?name=lis_cybercrime

Kiger, M. Arkin, O. and Stutzman, J. 2004. Profiling. In The Honeynet Project Know Your Enemy: Learning about Security Threats, Addison Wesley.

Kremen, S. H. 1998. Apprehending the Computer Hacker: The Collection and Use of Evidence, Computer Forensics Online. Retrieved 10 January 2017, from http://www.shk-dplc.com/cfo/articles/hack.htm

Levy, S. 1984. Hacker: Heroes of the Computer Revolution, New York: Bantam Doubleday Dell.

Li, X. 2006a. Economic Analysis of Cybersecurity: The Mixed Provision of Private Good, in John Roufagalas, ed. Resource Allocation and Institutions: Exploring in Economics, Finance and Law, Athens, Greece: ATINER, pp. 607-620.

Li, X. 2006b. Relative Concept of Cybersecurity, Information and Security: An International Journal, Volume 18, pp. 11-24.

Li, X. 2008. Cybercrime and Deterrence: Networking Legal Systems in the Networked Information Society, Turun yliopisto oikeustieteellisen tiedekunnan julkaisuja Rikos- ja prosessioikeus sarja, A: 34, Turku: Uniprint.

Maiwald, Eric. 2003. Network Security: A Beginner's Guide, second edition, California, USA: McGraw-Hill Osborne Media.

Ministry of Justice. 1985. Proceedings of Seminar on Problems of Computer Crime, Taipei: Communication of Justice Press.

Palczewski, C. H. 2001. Cyber-Movements, New Social Movements, and Counterpublics, in D. Brouwer and R. Asen. (eds.). Counterpublics and the State, New York: SUNY Press, 2001, pp. 161-186.

Parker, D. B. 1998. Fighting Computer Crime: A New Framework for Protecting Information, New York, N.Y.: John Wiley and Sons.

Philip, A. R. The Legal System and Ethics in Information Security, SANS Institute, 2002. Retrieved 10 January 2017, from http://www.securitydocs.com/go/1604

Pipkin, D. L. 2002. Halting the Hacker: A Practical Guide to Computer Security (with CD-ROM), Englewood Cliffs, New Jersey: Prentice Hall PTR.

Randall, K. Nicholas, Ryan, Denial J., and Ryan, Julie J. C. H. 2000. Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves, Columbus, USA: McGraw-Hill.

Schwartau, W. 1994. Information Warfare: Chaos on the Electronic Superhighway, New York: Thunder's Mouth Press.

Secretchina.com. Hebei Hacker Manuvored Sixty Thousand Computer to Create Cyber Bots, 17 March 2005. Retrieved 10 January 2017, from *http://kanzhongguo.com/news/pub/view.php?aid=89369*

Selwyn, N. and Gorard, S. 2001. 101 Key Ideas in Information Technology, United Kingdom, United States of America: Hodder and Stoughton-McGraw-Hill.

Smith, B. D. 1998. Psychology: Science and Understanding, Columbus, USA: McGraw-Hill.

Taylor, M. and Quayle, E. 2003. Child Pornography: An Internet Crime, East Sussex: Brunner-Routledge.

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.

Vatis, M. A. 1999. Congressional Statement, FBI, National Infrastructure Protection Centre (NIPC) Cyber Threat Assessment, Before the Subcommittee on Technology and Terrorism of the Senate Committee on the Judiciary, 6 October. Retrieved 10 January 2017, from *http://www.fas.org/irp///congress/1999_hr/nipc10-6.htm*

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.

Yan, W. and Zhang, Y. 6 November 2001. Xinjiang's First Cybercrime 17-Year-Old Hacker Arrested, Beijing Youth Daily.

Yi, M. 27 January 2006. Associated with Traditional Crime, Cybercrime Threats Citizens Safety, Huanghai Morning Newspaper.

Zheng, H. 2004. A Study on Cybercriminals, Social Sciences Front, number 6.