Aleksandre Glonti
Grigol Robakidze University
I level student of the Master's Programme in Law

Cybercrime Problem in Georgia and Foreign Countries

Brief History Introduction

As an object of scientific observation, cybercrime has its origins coming from the late 20th century, eventually when computers were invented. Now essential to modern life, computers and other Internet-connected devices have also become increasingly important to criminals who steal information, commit fraud and stalk victims online. Computers are used not only for committing crime but, thanks to the burgeoning science of digital evidence forensics, also to combat crime. During the period when computers became affordable, law enforcement agencies of the world faced the dawn of the IT era with growing concern about the deficiency of criminal laws available to combat computer crimes [9]. Eventually, massive popularization of computers resulted in the arousal of serious threats not only to banking operations, copyright and normal functioning of public services, but also to the national security [4]. According to the statement of FBI, the annual losses to the businesses in the United States alone estimated $67 billion and these numbers are still growing*".* Mirroring the international openness of the internet, cybercrime is a transnational phenomenon [8].

Definition of Cybercrime

Cybercrime, or computer crime, refers to any offence that involves computers or network. Cybercrimes are defined as "*Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical, financial or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet and mobile phones*". Computer crime captures within its scope a broad range of illegal activities. Generally, they may be divided into two main categories:

- Crimes that target computers directly
- Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device [11].

Majority of Cyber offences consist of spam, fraud, obscene or offensive content, harassment, drug trafficking, and cyber terrorism, cyber warfare.

High-Tech Criminals and how they use computers for criminal purposes

High-tech criminals, a.k.a. hackers, have also created their own crime courses. While some "old fashioned" delinquents seek the same ends as more traditional property offenders, modern technology

gives new age criminals (hackers) totally new criminal possibilities. They use computers to achieve their illegal sources of income, virus attacks and other cyber offences. Computer crimes are divided into three main categories:

First, the computer can be used as a storage or communication device whereby information can be created, stored, manipulated, and communicated electronically. In this instance, the computer is incidental, since it is not required for a crime itself but is used in some way that is connected to criminal activity; for example financial records that are kept on a drug dealer's computer.
Second, the computer can be used as an instrument or a tool of crime. In this case, the computer is used to commit traditional offences, such as the printing of fake money or forging official documents, or newer computer crime offences, such as the distribution of child pornography or phishing websites on the internet.
Finally, computer can be used as a weapon to commit attacks on the confidentiality, integrity, and availability of information, including theft of information, theft of services, and damage to computer systems. This type of computer crime involves the widespread problem of viruses and other forms of siege attacks, such as those referred to as "denial of service" (an attempt to make a computer or network resource unavailable to its intended users) attacks. It is often committed by so called "Cyber Vandals". An increasing number of electronic siege attacks employing some form of cybercrime have initiated against organizations world-wide in recent years [1].

International Legislation on Cybercrime

With the growth of computer crime, it has become necessary to implement regulative acts against cyber offences. In this period, several conventions took place and anti-cyber-crime legislations were adopted. However, despite the clear need for international cooperation on cybercrime, there is yet no genuinely global multilateral treaty (convention) dealing with this issue.
The Secretariat of the United Nations Office on Drugs and Crime (UNODC) prepared draft materials concerning cybercrime for the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. It has suggested that "the development of a global convention against cybercrime should be given a careful and a favorable consideration". But the United Nations Congress rejected a Russian-backed proposal of a treaty on cybercrime, despite widespread agreement that closer international cooperation is vital in a world more closely connected by global computer networks [13].

Currently, the main international convention on cybercrime is the Council of Europe's Convention on Cybercrime which was signed in Budapest in 2001 and forced in 2004. In 2010, the Convention on Cybercrime was signed by forty-six states and ratified by twenty-six. Though the Convention was drafted under the aegis of the Council of Europe, it is open for signature to non-members (the United States, Canada, Japan and South Africa). However, it cannot be referred to as a global convention. The Convention gives a list of crimes signatories of which are required to be implementing in their domestic law. The Council of Europe's Convention on Cybercrime has now been in force for more than seven years and has the widest coverage of any international agreement dealing with

cybercrime. The signature is open to countries which are not members of the Council of Europe, and four non-European countries have signed it already. Currently, scientists and scholars are discussing role of Convention on Cybercrime in development of legislative global standard.

Transnational Cybercrime

The traditional concepts and methods of terrorism have taken new dimensions, which are more destructive and deadly in nature. This new age terrorism is called "cyber terrorism". In the age of information technology the terrorists have acquired an experience to produce the most deadly combination of weapons and technology that will take its own toll, without proper attention from law enforcement agencies. The damage produced from cyber terrorism would be almost irreversible and most catastrophic in nature. The definition of "cyber terrorism" includes an intentional negative and harmful use of the information technologies for producing destructive effects to the property of others, whether tangible or intangible. For instance, hacking of a computer system and then deleting the useful and valuable business information of the rival competitor is a part and parcel of cyber terrorism.

The most widely cited paper on the issue of Cyber terrorism is Denning's Testimony before the Special Oversight Panel on Terrorism (Denning, 2000). Here, she makes the following statement: "Cyber terrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyber terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would serve as examples. Serious attacks against critical infrastructures could be acts of cyber terrorism, depending on their impact"[3].

There are four forms of cyber terrorism:

- **Secret information appropriation and data theft:** The information technology can be misused for appropriating the valuable Government secrets and data of private individuals and the State and its agencies.
- **Destroying of e-governance base:** The aim of e-governance is to make the interaction of the citizens with the government offices hassle free and to share information in a free and transparent manner.
- **Distributed denial of services attack:** The cyber terrorists may also use the method of distributed "denial of services" (DDOS) to overburden the Government and its agencies electronic bases. This is made possible by first infecting several unprotected computers by way of virus attacks and then taking control of them [6].
- **Network damage and disruptions:** The main aim of cyber terrorist activities is to cause networks damage and their disruptions. This activity may divert the attention of the security agencies for the time being thus giving the terrorists extra time and achieve their task comparatively easier. This process may involve a combination of computer tampering, virus attacks, hacking, etc.

Some Cybercrime Cases

Recent cyber-attacks have proved that even strongest firewalls (software protection against cybercrime) are sometimes ineffectual against professional hackers. A common axiom for any digital protection is that it can be always broken. Here are examples of most terrifying and costly cyber offences [10]:

1. US vs Osowski (2001) - Geoffrey Osowski and Wilson Tang were each sentenced today to 34 months in prison for exceeding their authorized access to the computer systems of Cisco Systems in order to illegally issue almost $8 million in Cisco stock to themselves.
2. Juvenile that was sentenced for successfully releasing a cyber-attack against Microsoft Corporation in 2005 [7].
3. Kevin Mitnick hacking IBM, Motorola, NEC, Nokia, Fujitsu Siemens and other corporations [1].

If such enormous software corporation, as Microsoft were victimized by the juvenile hacker, how can we be sure that someday a hacker with some mental disorders would not breach the nuclear weapon control panel?!

Cybercrime in Georgia

Process of computerization in Georgia started later than in Europe and North America. Personal computers were quite uncommon in houses of Georgians until the beginning of the 21st century. That is why the process of entry into era of cybercrime has been postponed in our country. Another factor which slowed impact of hi-tech criminality is lack of accessibility of Internet in Georgia.

Nevertheless, today we have already encountered some cyber offences, concerning copyright violations and software piracy issues. There were also several incidents related to website hacking. Such offences are leading to considerable economic loses. However, Georgians have not felt grave consequences of serious computer crimes such as cyber terrorism and cyber warfare, but unfortunately, this process is ongoing. In order to stop the further growth of cyberspace criminalization, Georgian law enforcement agencies must consider computer crime as a serious threat. If proper preventive, organizational and legislative measures are not adopted, in the nearest future Georgian economy and even national security might be endangered [2].

Penal Code of Georgia has chapter XXXV “COMPUTER CRIME” and chapter XXXVII “TERRORISM” that include 4 articles that are related to the cybercrime:

Article 284. Illegal Access to Computer Information - Illegal access to the computer information protected by law, i.e. the information reflected in data-carrier, computer, computer system or their network that has caused a loss, blocking, modifying or copying of information or malfunctioning of the computer, computer system or their network.

Article 285. Creation, Use or Circulation of Computer Damaging Programs - Creation of the program that damages computer or entering changes into the existing system that intentionally gives rise to any non-sanctioned loss, blockage, modification or copying of information or malfunctioning of the computer, computer system or their networks, as well as the use or spread of such program or a data-carrier replacing such program.

Article 286. Violation of Rule on Maintenance of Computer, Computer - Violation of the rule on maintenance of a computer, computer system or its network by the one who had access to the computer, computer system or their networks, that through negligence has caused a loss. Modification or copying of the computer information protected by law, or that has caused a substantial damage [5].

Article 324 (1). Cyber terrorism. Cyber terrorism is defined as "illegal acquisition of computer information protected by law, its use or threat of use, which poses the threat of grave results, and violates public security, state strategic, political or economic interest, committed with the purpose of coercing the population and/or influencing the state agency."

The article was amended to the Criminal Code in July 25, 2006 (amendment No.3530).

In 24 September 2010 Georgia Parliament adopted next amendments in Criminal Code:

- ✓ Criminal Liability of legal entities for cybercrime;
- ✓ Improved article concerning rights of intellectual property;
- ✓ Amendments were included in the article “child pornography”;
- ✓ Amendments were included in the article “illegal access to computing system”
- ✓ Amendments were included in the article “illegal usage of computer data or/and computer system”

Conclusion

High-tech crimes pose a special problem to law enforcement agencies of the whole world for two reasons. First, these crimes are not easily detected since the offenders can quietly commit them from any computer terminal, usually in comfort of their own homes. Second, while a few organizations have mobilized to attack high-tech crime, most law enforcement agencies are not equipped well enough to deal with this phenomenon. It is clear that the police forces of the future need to address this problem by concentrating on detection and by arming themselves with technological tools necessary to deal with it.

Modern Georgia lacks specialists in the field of cybercrime. Cyber criminals and cyber terrorists among them could use this factor to their advantage. No literature is available for next generations to learn from. This problem should be solved as soon as possible, before Georgians face grave problems.

References

1. Adler F., Mueller G, Laufer W. 2008. *Criminology and Criminal Justice System*. Edition 5th.
2. Alasania G. International Cooperation as a Strategy of Prevention and Fighting with terrorism in Georgia. *http://transcrime.cs.unitn.it/tc/fso/IMG%20altre%20iniziative/conference%20booklet%20washington.pdf*
3. Gordon S., Ford R. Cyberterrorism? Symantec Security Response. http://www.symantec.com/avcenter/reference/cyberterrorism.pdf
4. Harley B. A Global Convention on Cybercrime? on March 23rd, 2010. http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/
5. Tsatsanashvili M., Sikharulidze T. 2007. Law Problems of Cyber terrorism in Georgia. *Cybersecurity.* Tbilisi.
6. Criminal Code of Georgia. 2010.
7. Cyber Terrorism - The Dark Side of the Web World. http://www.legalserviceindia.com/article/l169-Cyber-Terrorism.html
8. FBI 2005 Internet crime survey. http://www.digitalriver.com/v2.0-img/operations/naievigi/site/media/pdf/FBIccs2005.pdf
9. Internet and Electronic Crimes. 11/05/2011 National Institute of Justice USA. http://nij.gov/topics/crime/internet-electronic/welcome.htm
10. United States Department of Justice – Computer Crime and Intellectual Property Section.
11. Wikipedia - http://en.wikipedia.org/wiki/Kevin_Mitnick
12. Understanding and Responding to Terrorism. 2007. *NATO – Security through Science,* Vol. 19,
13. http://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty