TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Irakli Benashvili

THE IMPACT OF CYBERCRIME AND LEGAL FRAMEWORK OF VOLUNTEERS IN CYBERSECURITY: CASE OF GEORGIA

Master's thesis
Law and technology

Supervisor: Agnes Kasper, PhD

Tallinn 2017

I declare that I have compiled the paper independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously been presented for grading.
The document length is 17 677 words from the introduction to the end of summary.

Irakli Benashvili ……………………………
(signature, date)
Student code: 156894HAJM
Student e-mail address: ibenashvili7@gmail.com

Supervisor: Agnes Kasper, PhD:
The paper conforms to requirements in force

……………………………………………
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
…………………………………
(name, signature, date)

Table of Contents

ABBREVIATIONS

BSI	Business Continuity Institute
CB	Caucasus Barometer
CDL	Cyber Defense League
CERT	Computer Emergency Response Team
COE	Centre of Excellence
CRRC	Caucasus Research Recourse Center
CSDC	Civil Society Development Concept
CSIRT	Computer Security Incident Response Teams
CSO	Civil Society Organizations
DAT	Defense Against Terrorism
DDOS	Distributed Denial of Service
DEA	Data Exchange Agency
EDL CU	Estonian Defense League's Cyber Unit
EU	European Union
EC	European Commission
IAVE	International Association of Volunteer Effort
ICT	Information and Communication Technology
ISAF	International Security Assistance Force
IT	Information Technology
LEPL	Legal Entity of Public Law
MECA	Middle East Cyber Army
MNCDE&T	Multinational Cyber Defense Education and Training Program
MNCD	The Multinational Cyber Defense Capability Development
MNMISP	Multinational Malware Information Sharing Platform
MOD	Ministry of Defense
NATO	North Atlantic Treaty Organization
NGO	Non-Governmental Organization
NSA	National Security Agency
SPS	Science for Peace and Security
UNDP	United Nations Development Program

ABSTRACT

Increase of use of electronic and computation technologies has brought with itself technical, as well as legal problems. Deterring cybercrime is an integral component of a national cybersecurity. The adoption of the legislation on national level against the activities which has a direct impact on the integrity of national critical infrastructure. It is a shared responsibility at the national level, which requires the coordinated actions from the government authorities and the private sectors to prevent and have an adequate response on the cybercrime.

The master thesis examines the current regulatory approach for cyber security at the national level and considers the applicable legislation in order to define and establish the legal nature of cyber security and volunteerism. The paper discusses whether Georgian approach to cyber security is compatible with EU and international standards. The analysis focus on the need of necessary amendments in the national law Georgian legislation into line with international standards. The thesis covers following research questions:

1. What is the legal nature of cybercrime in Georgia and is there a need to produce a new legislation to improve the cybersecurity?

2. Does the phenomena of volunteerism exist in Georgia and what is its legal status, how is it regulated?

3. Could Estonian practice provide legal solution to fill a gap in legal framework in Georgia regarding the cyber volunteers?

The thesis concludes volunteerism as a solution to develop defensive cyber capabilities and suggests the establishment of a voluntary organization in Georgia based on Estonian example.

Keywords: Cyber security, Cybercrime, Cyber defense, Volunteerism, Regulatory framework, Policy analyzing

INTRODUCTION

The marriage of the electronic programmable computer and widely available Internet over the last 20 to 25 years has changed the world as perhaps no other technology before. Worldwide use of Internet technologies is growing by leaps and bounds. More and more the internet is becoming integrated into modern life. The governments, the militaries, economy and the communications industry that helps human beings to stay in touch are also moving online. As a result, just about every industry, government and military is run by Internet-connected computers. This affords unprecedented efficiency, convenience and opportunity. The internet contributes to economic prosperity and growth, quality of life, access to information, social and political connection[1].

Wide application of internet has created positive developments in the social life. It appears to be easy to predict that every person will have the opportunity of using a computer and global networks in the nearest future. Technological revolutions, have not only stimulated progress in the society but have also become a motivation for previously unknown negative processes and developments. Alike many other revolutionary technologies, computer technologies bear enormous potential for the progress, as well as misuse. Complex and large-scale use of modern information technologies helps to shift humanity onto a new level of development. At the very beginning, computer was meant to be a gadget applied for calculation and computation purposes.[2] However, it has gradually turned into a unique and prodigious tool used by mankind for processing any kind of information. Modern world uses computers for managing banking systems, enterprises, defense area, spaceships. This means that there is no field of activities run by humans without using a computer. It is a tool for creating, collecting, storing, processing and transferring information.

However, the rapid Internet growth also creates new vulnerabilities. Now, countries must deal with new, more efficient threats coming from cyber space. Cyber-attacks are becoming more frequent, more organized and the cost of damage that they inflict on government administrations, businesses, economies and potentially also supply networks and other critical

[1] Denning, E. Cyber Conflict as an Emerging Social Phenomenon. Hershey: IGI Global, 2010, p 171-175

[2] Randell, B. On Alan Turning and the Origins of Digital Computers. Edinburgh: Edinburgh University Press, 1972, p 5-20

infrastructure is significant[3]. Modern information networks hold various information, including demographic and other data about ordinary citizens. The invention of strong electronic calculating technologies caused computerization of household and management activities, application of computer technologies in the fields of defense, atomic energy and other fields of civil life, where malfunctioning of such technologies may cause accidents and even disasters with loss of human lives and enormous economic damage.

In the 21st century, cyber-crimes become a central issue for the various countries. New technologies give origin to new crimes. Hence, with the invention of a computer, computer crimes became widely spread[4]. It is noteworthy that cybercrime has no borders. At the international level, it is important to have a coordination with the different partners. In 2013, one of the biggest cybercrime organization managed to steal 40 million USD from a bank. This case entails the breach of international law, company's internal policies and creates vulnerabilities that can lead to future incidents. Therefore, this has brought with itself technical, as well as legal problems. A harmful effect of computerization of society is a so-called "computer crimes", for instance, crimes committed through the internet and other computerized networks[5]. Computer crimes, such as network information intrusion, computer fraud, computer piracy, sabotage, electronic espionage, the spread of pornography and others have become regular problems.

One of the main problems regarding fight against cybercrime is that most of the information and communication networks is in property of private sector, when their safety is the responsibility of the State. The participation of private sector in this issue makes more difficulties to defend networks and protect of their security. Both groups, the government and the private sector have different interests and goals, which reduces the effectiveness of the protection of cyberspace[6]. This process becomes much more difficult when the issues interface becomes global, and significant role in the solution of above mentioned issue has international norms[7]. It may perform a catalytic role in the process, focus on harmonizing as national as

[3] Oconnell, M.E. Cyber Security without Cyber War. - Journal of conflict and security law, 2012, p 187-188

[4] Friis. K., Ringsmose J. Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives. Lancaster University, 2016, p 1-13

[5] Center for Strategic and International Studies. Net Losses: Estimating the Global Cost of Cybercrime. Said Business School, 2014, p 2-23

[6] Eichensehr, k.A. The Cyber-Law of Nations. - Georgetown Law Journal, 2015, p 320

[7] Simpson, B., Murphy, M. Cyber-privacy or Cyber-surveillance? Legal responses to fear in Cyberspace. Jurnal Information & Communications Technology Law. London: University of New London, 2014, p 189-191

international legal base and its perfection, where it is meant cybercriminal prosecutions, data storages protection, as well as providing network security and attacks against the principles of the security of network and operational response against cybercrime. However, there must be partnership between the public and private sector in the struggle against Cybercrime. There is also unanimity among states, international organizations, corporations and other sectors in the industry that collective measurements and cooperation with private sector is very important to achieve in this field.

When discussing cyber-crimes, it is important to mention one of the most important figures and phenomenon which is called volunteers and volunteerism in the cyber world[8]. Volunteers are nowadays one of the valuable resource. Volunteers are people who have specific knowledge and a desire to protect their country and, ones who want to contribute for their country by their own will, without any compensation. However, the issue is that the cyber volunteerism is not regulated by the law. It does not have a legal status. Thus, the lack of regulation does not allow to effectively use such resource as a volunteer in the field of cyber security. At the same time, there is experience of other countries, which will be discussed in this master thesis that work in this field and their experience can be applied. These people have huge potential to defend the country against potential cyber threats. The volunteers work on their own will, as already mentioned, without any compensation. Many of them prefer to stay anonymous. Some of these people are often working for governmental sectors. Cyber volunteers' actions are not regulated by the law in most of the cases, as they do not exist formally. This institute might be new for some countries however, in most of them, "volunteers" don't have the exact definition. The regulation of this phenomena is important as for individuals, as government sectors.

[8] Hadzi-Miceva.K, Comparative Analysis of European Legal Systems and Practices Regarding Volunteering. OECD Publications, p 1-23

1. HYPOTHESIS AND RESEARCH METHOD

In this master thesis author reviews the cybercrime as threat of 21st century. Analyses cyber dangers, strategies, and reviews volunteerism as a phenomenon in both countries in Georgia and Estonia.

Cybersecurity is a national security which means that the law enforcement issue is a primary responsibility for the government. What if the threat is invisible? When it is suddenly and virtually impossible to identify the source from which it comes? The development of modern technology has given many benefits to society, but it created a lot of new threats. According to the modern definition, cyber-attack is a deliberate attempt to impact the confidentiality, integrity and availability of computer networks and electronic services[9]. Such action may be aimed at damaging or delaying the service, as well as the use of computer networks for offensive purposes, such as information and database leakage and provision of unauthorized access to it in the future.

In August 2008 Georgia became the target of such cyber-attacks. As a result, attacks were blocked Internet - communication, public servers had been damaged, destroyed a web - pages, fake websites have been created. Computers of Georgian banks were overwhelmed attempts dangerous transactions which forced foreign commercial institutions to block, for security purposes, contacts with the Georgian side. The culmination was the DDoS-attack six botnets that used computers of unsuspecting Internet users and volunteers, download the program for breaking from several anti-Georgian websites[10]. This showed the necessity to attract and train new professionals who can fight back invisible threat. Such experts may be volunteers, people who have specific knowledge and a desire to protect their country. But the main issue is that there is not available legislation that regulates their activities and determine the legal status. The lack of legal regulation does not allow to effectively use such resource as a volunteer in the field of Cyber Security.

[9] Appazov, A. Legal Aspects of Cybersecurity. Copenhagen: Faculty of Law University of Copenhagen, 2014, p 14-17

[10] Tarkhnishvili, N. Two “Keys” is Still Controversial. Tbilisi: Radio Liberty, 2015, p 2-8

The hypothesis of this thesis is that current Georgian regulation needs to be modified or new legislation established to bring it into line with international standards. In addition, establishing cyber volunteer organization and regulating the volunteerism can help to improve the cyber security level in Georgia. The author believes that by establishing the cyber volunteer organization and by regulating the cyber volunteerism the country can improve the cyber security level.

The thesis consists of four main chapters and starts with explaining the research aim and methodology. The thesis then continues to define the specific issues circulating the cyber security. The second chapter focuses on important aspects of cybercrime and cybersecurity in Georgia, showing the importance of a cybercrime on national and international level. The third chapter of the thesis defines the existing concepts and laws applicable in Georgia, considers legal challenges in Georgian cyber security and the current regulatory approaches in the country. The fourth chapter focuses on the role of cyber volunteers, brings the theoretical models for volunteerism on cyber militias and compares the regulatory framework for volunteerism in Georgia and Estonia. The Chapter proposes possible solutions in regulatory scheme to improve cyber security level in Georgia and gives an insider perspective on the current situation. The author finally drafts a conclusion on the Georgian regulatory approach.

The master research will provide Estonia's experience in the field of cooperation with cyber volunteers. Discuss the prospects of cooperation and cyber volunteering for Georgia on the example of Estonia. With this context, the research investigates on the legal status of volunteers in national law, responsibility and security guarantees. Including the case studies and legal framework of volunteers in national and international level, legislative framework and legal status of volunteers in Georgian law. The author has used qualitative research methods to prove the hypothesis and answer the research questions. The author has analyzed academic materials as well as legislation gathered on the topic to answer the research questions and prove the hypothesis. In addition, the work includes a comparative analysis based on the different legislative regimes of Georgia and Estonia to look into the legal challenges surrounding Georgian legal framework and find possible solutions.

1.2. Literature Review

Most of the existing academic and policy related literature with respect to the cybercrime and cyber security starts out by discussing the rise of the Information Age and the centrality of the information and communication technologies in almost all sectors of the society from government, business and even including the individual level. Information has always been important, however, in postindustrial society, it became even more paramount, accessible and vulnerable· The dependence of the society on information systems dramatically increases with many activities having a network enabled capacity. Therefore, the potential damage of cyber-attacks is quite large. One of the greatest threats coming from these attacks target critical infrastructure assets, which includes telecommunications, financial services and defense. The attacks can be economically damaging and disruptive and cyber-attacks on critical infrastructure became quite common. With there being a plurality of attacks such as espionage, destruction of critical information systems the desire for having a secure cyberspace is growing amongst governments as well as amongst non-state actors[11].

Despite the development of offensive cyber capabilities by various states and the number of the importance of the cyber threats, the issue has not been fully addresses on a truly global level.[12] It has been widely recognized that the lack of clear and widely excepted definitions on concepts relevant to cyber threats has been one of the main hurdles in developing global agreements on cyber security. Clearer definitions on different types of cyber-attacks and international norm setting is important when dealing with already existing international agreements. It is not very clear whether cyber-attacks should be viewed as aggression covered under the UN Charter Article 51, under the solidarity clause in the Lisbon Treaty or under the Article 5 of the NATO treaty[13]. In case, if cyber space be reviewed as the fifth domain of defense together with land, sea, air and space, the cyber-attacks could possibly be considered as kinetic attacks.

Furthermore, there has been virtually no literature which would be directly relating the implications of cyber security to international relations as well as to legal theory. Most of the

[11] Gamreklidze, E. Cyber security in developing countries, a digital divide issue. – Journal of international communication, Vol. 20, 2014, p 200-217

[12] *Ibid.,* 211

[13] Charter of the United Nations. United Nations. 1 UNTS XVI, 1945 www.unwebsite.com/charter (12.12.2017)

literature about the cyber security has been written by or aimed at policy makers and therefore has not gone over any major theoretical considerations. Most of the literature available is pragmatic in nature with a little to no theoretical considerations. Although, as a result of the importance of the issue and the literature used in this master thesis indicates that the amount of academic work done on it is growing. Yet there is a large consensus with respect to the types of cyber threats and attacks, even though the scale and severity of the threats are still subject to debate.[14] Moreover, there is still an international agreement such as Convention on Cybercrime, regarding the need for a global response in order to effectively and adequately combat the cyber-attacks.[15]

[14] Gercke, M. Understanding cybercrime: Phenomena, challenges and legal response. The ITU publication, 2012, p 1-4

[15] Convention on Cybercrime. Council of Europe Treaty Office. No. 185, 2001. www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (20.09.2017)

2. IMPORTANT ASPECTS OF CYBERCRIME AND CYBERSECURITY: CASE OF GEORGIA

2.1. The Phenomena of Cybercrime

Deterring cybercrime is an integral part of a national cybersecurity and critical information protection strategy. This includes adopting an appropriate legislation at the national as well as at the international level. In most of the reports, guides or publications the cybercrime is being defined by the terms "computer crime" and "cybercrime". In this context, as it is discussed in this master thesis below, there have been several approaches adopted during the recent decades in order to develop a specific definition for both terms. However, before evaluating the approaches, it is important to determine the relationship between cybercrime and cyber-related crimes. The term "cybercrime" in has a narrower meaning comparting to computer-related crimes. As it has to involve a computer network. Whereas, computer-related crimes involve the offences that bear no relation to a network, but only effect stand-alone computer systems.[16] Two definitions have been developed during the 10th United Nations Congress on the prevention for Crime and the Treatment of Offenders. Cybercrime in a narrow sense "(computer crime) covers any illegal behavior directed by means of electronic operations that target the security of computer systems and the data processed by them"[17]. And cybercrime in a broader sense "(computer-related crimes) entails any illegal behaviors committed by means of, or in relation to, a computer system or network which includes such crimes as illegal possession and offering or distributing information by means of a computer system or network"[18]. There is also a common definition that describes cybercrime as any activity in which computers or networks are a tool, a target or a place of criminal activity.[19] However, this broad definition has several issues. For instance, it would cover crimes such as murder, if perchance the offender used a keyboard to kill the victim. Another broad definition is mentioned in the Article 1.1 of the Stanford Draft International Convention to Enhance

[16] Gercke, M. Understanding cybercrime: Phenomena, challenges and legal response. The ITU publication, 2012, p 11

[17] Kaur, N. Prevention and Control of Cyber Crimes. Journal of Computer Science and Engineering*,* 2016, p 37

[18] *Ibid.*

[19] Gercke, M. Understanding cybercrime: Phenomena, challenges and legal response. The ITU publication, 2012, p 11

Protection from Crime and Terrorism. The definition mentions that cybercrime refers to acts in respect to cyber systems.[20]

Some other definitions try to take objectives or intentions into account and define cybercrime more precisely such as "computer-related activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"[21]. Thus, this definition excludes cases where physical hardware is used to commit regular crime, but they risk excluding crimes that are considered as cybercrime in international agreements such as the Commonwealth Model Law on Computer and Computer-related Crime or the Council of Europe Convention on Cybercrime. Thus, the number of approaches demonstrate that there are considerable difficulties in defining "computer crime" and "cybercrime". As computer crimes differ in many ways, the single criterion does not exist that could include all the acts mentioned in the different legal approaches to address the issue.

Without human users, cyberspace would stagnate, fall into disrepair and eventually – cease to be. Unless something else can take over the maintenance and development of cyber infrastructure and content, the human remains an important part of cyberspace.[22] On the defensive side, in cyberspace it is possible to upgrade defenses in seconds or minutes by implementing new firewall rules, for example. Building a new concrete bunker or a Maginot line in physical space is much more time consuming. Though, this does not mean that erecting defenses in cyberspace is or can always be done in minutes. It merely points out that it is possible to deploy prepared defensive measures (tighter firewall rules, alternative routing and hosting etc.) in a short amount of time.[23]

Computer crime is common to every state establishing computerized governmental structures. Such criminal pursuits are particularly spread in management and industrial systems, banking and service-related activities. There exists variety of activities and outcomes resulting from illegal use of computation technologies. There is a list of main types of computer crime relating

[20]*Ibid.*

[21] Friis, k., Ringsmose, J. Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives. Abingdon: Routledge, 2016, p 225

[22] Ottis, R. (2011) Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability, www.ccdcoe.org/multimedia/theoretical-model-creating-nation-state-level-offensive-cyber-capability.html (18.12.2017), 2011, p 1-7

[23] *Ibid.*

to such misdeeds, for instance, unauthorized access to computer storing information; insertion of a “logic bomb” into a software support that will set off a malicious function when specified conditions are met, resulting in partial or full breakdown of computer system; developing and spreading computer viruses; forge and spoliation of computer information[24]. Terrorists’ raids on computer centers, electronic fraud in various networks used for money transfer, viruses and false programs, corporate espionage among commercial computer networks, so-called “computer hooligans” attempting to illegally access computer networks using internet – all of the above represent a sad reality[25]. Notwithstanding the numerous precedents, the theories relating to the essence of computer crime are not clearly developed until now. Its complexity, is due to inability to define a unified object of infringement and a variety of issues. Many types of crimes, due to the increase use of computation equipment, have been modified. Therefore, we may only consider computer aspects of crime and not a computer crime itself. Cybercriminals target public and private persons’ interests. Total loss caused to the USA’s state and commercial structures because of computer crimes amounted to approximately 400 million US dollars.[26]

The level of computer crime is higher in the countries, which stands out with high level of automation, and development of technique. Consequently, these countries have accumulated more experience in fighting against cybercrime, where the typology of computer crimes, as well as persons committing it is studied and analyzed along with developing the methodologies for security against such crimes. The term “computer crime” first appeared in the US scientific sources already in 50-60ies in the 20th century[27]. So, we can say that electronic computer was and is the best universal tool for committed intended crime. Nowadays, social and moral damaged caused by cybercrimes is countless[28]. Moreover, high latency of such crimes, for instance, only about 10-15% of computer crimes are known as the companies affected try not

[24] *Ibid.*

[25] *Ibid.*

[26] Center for Strategic and International Studies. The Economic Impact of Cybercrime and Cyber Espionage, www.csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf (29.10.2017), 2013, p. 1-15

[27] Wild, Ch., Weinstein, S., MacEwan, N., Geach, N. Electronic and mobile commerce law: an analysis of trade, finance, media, and cybercrime in the digital age. Hertfordshire: University of Hertfordshire Press, 2011, p 309-314

[28] Jayakumar, Sh. State, Society and National Security: Challenges and Opportunities in the 21st Century. Singapore: World Scientific Publishing, 2016, p 215-247

to disclose about such crimes committed fearing that this could possible negatively affect their reputation and/or impulse repeated committing of computer crime against them[29].

From authors point of view, Legal norms relating to computer crime are, firstly, developed for ensuring information protection. The norms regulating legal aspects of operating computer technologies are included in various subjects of law. Criminal law has particular importance among various legal instruments for civil relations. Criminal law explicitly defines the activities to be considered a crime, as well as types of punishment for a person committing it[30]. Cybercrimes are not treated uniformly. In some countries, unauthorized access is a crime only of harmful intent is present. In other cases, data theft is a crime only if data relates specifically to an individual's religion or health, or if the intent is to defraud. Despite the progress made in the legislation for many countries, many of them still rely on standard terrestrial law to prosecute cybercrimes. This means that, many of them are relying on archaic statutes that predate the birth of cyberspace and have not been tested in court. In addition, the weak penalties in criminal statutes provide limited deterrence for crimes that can have a large-scale economic and social impacts. Countries in the developing world are seeking a model to follow. Although, only few of them have a legal and technical resources necessary to address the complicities of adapting terrestrial criminal statutes to cyberspace. Therefore, it is necessary to have a public-private partnership in order to produce a model approach which can help to eliminate the potential threats[31].

Computer systems are increasingly affecting social life. Malfunctioning of computers, computer systems and their networks can lead to destructive result. For instance, in 2013 a gang of cyber-criminals stole $45 million by hacking into a database of prepaid debit cards[32]. Enormous amount of information is being stored by computers and their networks around the world. Computer networks hold also information relating to scientific researches, rule of law, state secrecy. Currently, under the circumstances of globalization there is no field where

[29] *Ibid.,* 217

[30] Jahankhani, H., Nemrat, A., Far, A. Cybercrime classification and Characteristics. Cyber Crime and Cyber Terrorism Investigator's Handbook, 2014, p 149 -162

[31] Crandall, M. Soft Security Threats and Small States: The Case of Estonia. - Defense studies Journal, 2014, p 30-55

[32] Reuters reporter. Seven cyber hackers 'stole $45 million in just 10 hours' by draining cash machines in one of world's biggest ever bank heists, 2013 www.dailymail.co.uk/news/article-2322062/Seven-cyber-hackers-caught-stealing-45-million-10-hours-second-biggest-bank-robbery-history-New-York.html (21.11.2017)

computer is not necessary. Criminal law of any developed or developing country around the world puts emphasis on fight against cybercrime. Therefore, legislations define criminal responsibilities for any possible deed. Limitless potential of computation technologies points to the fact that current situation is a beginning of this dangerous and threatening problem. Moreover, when technologies are developing so fast and there are so many scientific and technical progress, computer crime, is turning into one of the most dangerous crimes among all. Computer crimes cause particular threats to the field of finance. Criminal groups steal millions by means of illegal use of new technologies, get rid of taxes and carry out complex works for preparing and committing new crimes. Cybercrime on international level has clearly exceeded other types of crime and its prevention becomes almost impossible.

Georgia is a party to the Treaty of Organization of the Black Sea Economic Cooperation on fighting against crime, also signed by Albania, Azerbaijan, Bulgaria, Moldova, Romania, Russia, Turkey, Armenia and Ukraine. The parties have agreed upon cooperating in fight against particularly grave crimes, among them crimes in the field of high technologies, including cybercrime.[33] Gradually, it became necessary to develop complex international measures for preventing incidents relating to the exchange of information for the creation of an international legal data base, aiming at protecting destructive use of information resources of national and global level. The initiative and resolution of the vice president of Georgia Mr. Mikhail Saakashvili signing the Convention on Cybercrime of the Council of Europe that was adopted in Budapest on 23rd November 2001 was another step forward in the field of fight against cybercrime and harmonization of Georgian legislation with international and European legislation[34]. Main aim of the member States of the Council of Europe and the other signatory countries is to achieve unity between its members, also recognizing the value of fostering co-operation with the other States parties to this Convention. Important aspect of common criminal policy is protection of society from cyber-crime, by adopting appropriate legislation and fostering international co-operation.

Development of computers, electro techniques and continuing globalization of computer networks brought as many risks as benefits. Computer networks and electronic information

[33] Sabanci Cad S., Fuad Paşa Yalısı M., Tersane E., Organization of the Black Sea Economic Cooperation, Permanent International Secretariat. www.osce.org/cio/128791?download=true (23.04.2017), p 1-9

[34] Convention on Cybercrime. Council of Europe Treaty Office. No. 185, 2001
www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (20.09.2017)

may also be used for committing criminal offences and the evidence of that criminal offences can be stored and transferred by these networks. Each of signatory countries considering and recognizing importance and need of co-operation between states and private industry in struggle with cyber-crime. They believe that effective fight against cybercrime requires increased, rapid and well- functioning international co-operation in criminal matters.[35]

Computer crime in Georgia became particularly resonant after the August developments, where Russian Special Forces and special groups attacked Georgian internet space causing tremendous, one could even say irremediable damage to it[36]. David M. Hollis, who is analyst with the Office of the Undersecretary of Defense and Army Reserve officer with U.S. Cyber Command describes how the Government of Russia involved cyber operations in its plans against Georgia. "In spite of Russia's evident attacking cyber operations during the August war, they were concealed by involving third party and creating a route for attacking using wide spectrum of server synergies, that is a common practice for cyber operations.[37]" The Report of the Government of Georgia on a full-scale aggression of the Russian Federation against Georgia mentions that "Russia has applied six ways of fighting a war against Georgia: land, air, naval, missile forces, cyber-attacks and media war".[38] Since then, significant changes were observed with regards to this issue. For example, a working meeting was held at the Ministry of Justice of Georgia referring the EU-funded computer crime project on March 2, 2010. Computer crime project aimed at supporting safety of information and communication technologies is Georgia. The project envisaged implementation of various reforms, including development of relevant legislation, capacity building of special target groups through trainings etc.[39] However, relevant normative and institutional basis for fighting against computer crime should be developed, as well as relevant qualified human resources ensuring safety of the country in this field.

[35] Brenner, S. Cybercrime: Criminal Threats from Cyberspace. Santa Barbara: Praeger, 2010, p 14-21

[36] Carr, J, Inside Cyber Warfare. 2nd ed. Town of Newton: O'Reilly Media, 2011, p 3

[37] Report of the Government of Georgia, Full-scale Aggression of the Russian Federation against Georgia, www.civil.ge/files/files/GeorgianGovernmentReportWar.pdf (22.02.2017), 2009, p 17

[38] *Ibid.*

[39] Council of Europe, Project on Cybercrime, www.rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa379 (22.02 2017), 2010

Extending the rule of law into cyberspace is very important and a critical step to create a safe environment for people and for businesses. The extension is still in process in many countries, including Georgia. Thus, the organizations should defend their own systems and information from attack, be the threats coming from outsiders of from within. The organizations may rely only secondarily on the deterrence that effective law enforcement can provide. To provide the self-protection, the main focus should be on the implementation of cyber security plans which will address technology related issues. The public and private sector employees should receive education on security practices, develop thorough plans for the handling of sensitive data, records and transactions. Different robust security technology, such as anti-virus software, authentication services should be incorporated throughout the computer systems. However, the main issue is that these software and hardware protection tools for defending information systems are expensive to operate. As national governments remain the dominant authority for regulating a criminal behavior, it is important to examine current laws to distinguish if they are composed in a technologically neutral manner that would include the prosecution of cyber criminals. The adoption of enforceable laws regarding the computer crime that respect the rights of individuals are an essential to fight against the cybercrime.

2.2. Cyber Crime and Cyber Espionage

From 2014 Georgia has started to collect the official statistics on cybercrime. The data is provided by the Information-Analytical Department of the Ministry of Internal Affairs (MIA) of Georgia. Despite the fact that there is no official statistics available before 2014, the CCD of the Central Criminal Police Department (CCPD) has investigated more than 30 cases of cybercrime[40].

The Annex I presents the numbers of registered and resolved cybercrimes during the year 2014 including the first half of 2015 by the MIA territorial and structural united under the articles 284-286 of the Criminal Code of Georgia. Article 284 provides the illegal access to a computer system; article 285 mentions the misuse of a computer system or/and creation, usage, and

[40] Dowling, S., McGuire, M. Cyber Crime: A review of the Evidence. London: United Kingdom, Home Office, 2013, p 1-30

dissemination of malicious computer programs; and finally, article 286 discusses the computer system interference and/or computer data corruption, modification and deletion[41].

According to the statistics provided by MIA, during the year 2014 and first half of 2015, the cybercrime under the article 255 has not been recorded. The article 255.1 of the Criminal Code discusses the involvement of a minor in creation and sale of pornographic products or products of such a nature. Furthermore, there the statistics under number of articles available to MIA such as Article 180 which is about the fraud, unlawful appropriation of property or property rights through deception; Article 189 infringement of copyright or related rights; Article 210, forgery, sale, use, abuse of credit cards or other payment methods. The reason for the absence of this statistics is that MIA did not keep these statistics before and the Ministry still needs to work out of an accurate methodology to provide reporting. Investigating the violations committed under Article 324.1 of the Criminal Code, is a responsibility of the Counterterrorism Center of the State Security Service, which for previously part of MIA. The Article discusses about the counterterrorism.

The numbers provided by the MIA likely reflect underreporting, which could cause by several factors. Firstly, in Georgia the overall level of cybercrime awareness is very low among public and government officials not directly charged with cybersecurity[42]. For instance, news on cyberattacks is actively discussed and is leading topic in foreign press. However, in Georgia there is not much discussions on this issue. The result of the lack of general awareness can be that many people are victimized without even knowing about it. Secondly, when there is a case of the loss for small account-holders, the banks are ready to reimburse the amount without reporting such cases to the police. Thus, as the number of such cyber-crimes increase, it is very important to have a better reporting and recording systems. In addition, although law obliges private companies to report the crimes, there does not exist any mechanism to check if the report such crimes.

There are many cases of cyber war and cyber espionage in different countries and Georgia is no exception. Cyber espionage and cyber war might seem to rest apart from cybercrime. However, if we take Georgia as an example, it showed that these three are should be understood together.

[41] Criminal Code of Georgia. Parliament of Georgia. Legislative Herald of Georgia, Tbilisi, Georgia. No. 2287, 22.07.1999

[42] The Report of the Government of Georgia. A Full-scale aggression of the Russian Federation against Georgia. www.civil.ge/files/files/GeorgianGovernmentReportWar.pdf (23.03.2017), 2009, p 1-39

Cyber espionage is a crime and combating this act has a higher priority among Georgian officials competing to cybercrime itself. This reasoning is based on the documents such as the National Security Concept of Georgia[43]. The country has been a target of cyber espionage and cyber-attacked directed from Russian cyber-criminals. It is very important to understand that the threats are coming from a group-or groups composed of Russian cyber-criminals.

In 2008, Georgia has experienced combined kinetic and cyber-attacked coming from Russia. The United States Cyber Consequences Unit (US-CCU), which represents and independent research institute reported that many of those attacked were so close in time to the military operations that it gave a reason to assume that there was a close cooperation between in Russian military and civilian cyber-attack. The US CCU report underlines that there was a clear evidence of the involvement of Russian Business Network, a cyber-criminal syndicate. The 2008 Cyber-attacks effected Georgian government's information and communication sector, various news portals, financial transactions and Internet traffic which lasted for several days[44].

Another tool that was used in 2008 from cyber-criminals was web posting of instructions to individuals who did not have enough computer skills to determine the risks. These individuals were used as a tool to contribute the cyber-attacks. This was so effective that nearly forty targeted websites were effectively shut down. Several social networks and webpages were also used for recruitment purposes.

2.3. Securitization and How Georgia Views Cybercrime

The main concept of securitization provides a benchmark on how intensely nations perceive security related issues. This concept was established by Arnold Wolfers in 1950 and later employed by Barry Buzan in 1997[45]. It is described as a process by which a country deals with a threat outside normal channels, which is not technical or legal matter, but rather as an existential threat which is warranting extraordinary attention. Good example could be a nuclear deterrence in the Cold War and the war on terrorism[46].

[43] The Report of the Government of Georgia. A Full-scale aggression of the Russian Federation against Georgia. www.civil.ge/files/files/GeorgianGovernmentReportWar.pdf (23.03.2017), 2009, p 1-39

[44] *Ibid.*

[45] Buzan, B. Rethinking Security after the Cold War. Cooperation and Conflict. California: SAGE Publications, 1997, p 5-28

[46] *Ibid.*

Even though the cyber treats and 2008 cyber-attack had a direct impact on Georgian national security, this issue is not yet fully securitized. It remains one of the main challenges country faces, dealt by legislation, bureaucracies and including country's budget. After the 2008 attack, Georgia indeed has implemented many steps and improved the its capabilities for cyber security. However, there needs to be done much more in this respect as securing the country's cyber space is one of the most important matters. The cyber security has indeed high priority for the country, however, there should be sufficient budget to match with the declaratory policy. For instance, Georgian government computer systems are running unlicensed software and replacing all the government owned computer systems would include high costs. Based on the Software Alliance BSA, 2014 Global Software Survey rated countries using unlicensed software installation where Georgia had a 90% of rate, which is very high. This number constitutes very important commercial value of approximately 40 million[47].

According to the report issued by the Eurasia Partnership Foundation, private software is widespread in public as well as in private sectors. Based on the report, in central and local government most of the personal computers which consist of 70% are run by the unlicensed or so called pirated software. Furthermore, the National Intellectual Property Center called Sakpatenti, there have been ongoing negotiations between the government of Georgia and Microsoft to solve the issued, with a view toward introduction of licensed software in government agencies[48]. However, as discussed above, the main obstacle is related to financial resources.

Protection of intellectual property rights (IPR) is closely linked and has a significant importance for Georgia's development in the ITC sector and beyond it. Georgia has implemented new laws which lead to bring its IPR legislation into line with international standards. The Georgian National IPR center – Sakpatenti, is the agency which is formulating and implementing IPR-related policies. Starting from 2014, Georgia has ratified some various international conventions with respect to the IPR, amended existing IPR laws on trademarks, patents, copyrights and other related rights. This helped to harmonize Georgian legislation with EU and international standards.

Thus, based on the analyses provided above and after reading the emphasis placed on cyber security it is a fact that cyber security has a high priority in Georgia, especially after the 2008

[47] Gamreklidze, E. Cyber security in developing countries, a digital divide issue. – Journal of international communication, Vol. 20, 2014, p 200-217

[48] *Ibid.,* 215

events. However, there is still insufficient understanding beyond the government cyber security community, including the insufficient funding in order to fix some major issues.

Only efficient policing is not enough for a law enforcement system to work, the role of prosecutors and courts has a significant importance. However, there is a lack of understanding of cyber technology among Georgian prosecutors and court officials which has crated concern in Data Exchange Agency (DEA) and the Cyber Crime Division (CCD). CCD has reported that prosecutors and judges have a lack understanding of cyber cases. According to CCD there have been several cases in which, despite the solid evidence and evidence procedures, the final verdict was not appropriate as a result of judge's lack understanding of the case.   To address, the issue, DEA has offered training for prosecutors. The training included topics related to cyber space, cyber security and cyber law. There were only a few attendees from the prosecutor's office and number of them dropped the training course as it was too complicated for them[49]. This gap needs to be filled as it is hard to process the cyber cases as fully understanding the technical sides of those cases can be challenging.

[49] The Russo-Georgian War 2008: The Role of the cyber-attacks in the conflict, www.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf (23.04.2017)

3. CONCEPTS AND LAWS IN GEORGIA: ANALYSES OF LEGAL FRAMEWORK ON CYBERCRIME

3.1. National Security Concept and Law on Information Security

In 2008, during Russian-Georgian war, the Russian Federation together with the ground, air and naval attacks has conducted large-scale cyber-attacks. This was showed the importance of the protection of cyberspace in terms of national security. The security of cyber space has a significant importance for Georgia. With the evolvement of the information technologies, critical infrastructure is becoming more dependent on them. Thus, fighting against cybercrime and protecting against cyber-attacks has a major importance to the national interests of Georgia. On June 6 of 2012, Georgia has ratified the European Convention on Cyber Crime. The treaty was signed in 2008 and it requires not only cross-border law enforcement cooperation, but also harmonization of certain laws pertaining to cybercrime. This required time, therefore ratification was not possible until Georgia passes its Law on Information Security. Starting from October 1st of 2012, the European Convention entered into force for Georgia[50].

During the years of 2008 and 2009, the MIA was actively involved in the joint project with the Council of Europe and European Commission on Cybercrime. This project aimed to harmonize Georgian legislation with Cybercrime Convention. Within the framework of this project very important amendments were made in Georgian Criminal Code and the Law on Criminal Procedure. The review and amendment of the laws is still ongoing process and is necessary in order to bring greater clarity and conformity with the convention. Similar to any country, Georgia must adapt its laws to relatively new international agreement and adapt to new technology. The country still needs to modernize its legal system with together with the practical experience and with foreign assistance.

The law on information security is applicable to legal persons and state agencies recognized as critical information system subjects. Georgia has made a number of amendments to the law during the years of 2014-2015. Therefore, the new list of critical information system subjects and its categorization which includes the field of defense, is approved by an order of the

[50] Convention on Cybercrime. Council of Europe Treaty Office. No. 185, 2001 www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (20.09.2017)

Government of Georgia. According to the procedure, the Ministry of Justice, along with the Ministries of Defense and the International Affairs and State Security Service submits a draft order with the Government of Georgia for the approval. Before this amendment was incorporated, the list was defined by a decree of the President of Georgia, based upon a list provided by the National Security Council. Another amendment which was made to the law lead the creation of the Cyber Security Bureau (CSB) as a legal entity of the public law. CSB is under the supervision of the Ministry of Defense[51].

The law sets out different obligations and requirements to be fulfilled for critical information system subjects such as for instance, to adopt information security policies which is compliant with the ISO 27000 and standards set by the Information Security Audit and Control Association (ISACA). The organizations included in the list of critical information system subjects also require appointing the information security officers including cyber security personnel. In addition, these organizations are responsible to conduct information asset management in order to categorize the assets in terms of their criticality. The law also authorizes critical information subjects to conduct information security audits, also to undergo the penetration testing and manage a network sensor for the detection of cyber-crimes. The law defines the competences of the Georgian CERT as a national CERT and discusses its interaction and exchange of data with owners of critical information systems.

The DEA does not have a direct access to the critical information system subject's information systems, including the information assets. It can only have an access in case if subject voluntarily will provide DEA with the access. Information security manager of a critical information system subject is responsible to inform the CERT of computer incidents. However, on the other hand, the subject has a right to make a decision whether to accept the CERT's assistance or not. The CERT would not have a right to have an access on a subject's data without this permission[52]. Any legal entity and state agency which is not a critical information system subject has a right to voluntarily implement information security mechanisms which is given by the legislation. This law is not applicable to mass media, publishing companies, scientific, educational, religious and community organizations, including political parties.

[51] Law of Georgia on Information Security. Parliament of Georgia. Legislative Herald of Georgia, Tbilisi, Georgia. No. 6391, 2012

[52] Tarkhnishvili, N. Two "Keys" is Still Controversial. Tbilisi: Radio Liberty, 2015, p 4-11

The law entails various sub-normative acts which defines and develop the legal provisions for the further implementation. There are different orders on for instance, Computer Emergency Response Team (CERT) of the Data Exchange Agency; approval of minimum standards for an information security officer of a critical information system subject; configuration of network sensors in the networks of the critical information system subjects; minimum requirements of information security; approval of rules for authorization of persons and organizations eligible to perform information security audits, authorization procedures and costa; rules for conducting an information security audit; approval of rules on information assets management. There are three orders for MoD Cyber Security Bureau, such as: Computer Security Incident Response Team (CSIRT), minimal requirements of information security and rules for information asset management[53].

The CCS has the authority to define the requirements for the critical information system subjects in the field of defense in accordance with the conditions and requirements which are provided by the ISO and ISACA.

The amendment made in the law was mandatory in order to strengthen the implementation of regulations which pertain to ensure the protection of confidential and internal use of the information at the critical information system subjects. On 29 April of 2014 the Government has approved the updated list of the critical information system subjects which included 39 organizations[54].

With the Law on Information Security, Georgia has successfully conformed to the European Convention. Despite this, there are number of issues that arise in connection with this law. The first issue to point out is with respect to achieving a good government-industry partnership. Government officials assessed private business to be reluctant to cooperate. And another issue is regarding the creation of well trained professionals who will assist to implement the law fully. It is important to mention that in Georgia it is a problem to find a university that can give a quality education in the field of computer science or cyber security. At the moment, the existing universities do not have such capabilities. However, the progress to solve this problem is visible. This has a direct effect on the implementation process of the information security

[53] Tsatsanashvili, M. "Information Law". Tbilisi: Tbilisi Publishing Limited, 2014, p 8

[54] Georgian Law on Personal Data Protection. Parliament of Georgia. Legislative Herald of Georgia Tbilisi, Georgia. No. 5669, 2015

law as there is not enough cyber security personnel to follow all the requirements that are indicated in the law. All the defined organizations need 2-3 professionals working the problem.

3.2. Criminal Code and Changes in the Laws on Electronic Surveillance

The Criminal Code of Georgia regulates the cybercrime by the Chapters 25,27,32,35 and 38, according to which, criminal responsibility is established for committing the illegal acts in cyberspace such as for instance, illegal access to computer system, which is provided by the Article 284[55]. Misuse of a computer system and/or creation, usage and dissemination of malicious computer programs (Article 285). Computer system interference or/and computer data corruption, modification and deletion (Article 286). Offering to provide child pornography in any form or/and illegal creation and dissemination of pornographic materials (Article 255). Involvement and engagement of a minor in creation and sale f pornographic products or products of a pornographic nature (Article 255.1). Infringement of copyright or related rights (Article 189). Cyber terrorism (Article 324.1). Forgery, sale, use, abuse of credit cards or other payment cards (Article 210). Froud, that is, unlawful appropriation of property or property rights through deception (Article 180).

Article 324 regarding the cyber terrorism has been amended earlier in 2012 following the amendment of the articles 255 and 255.1 in the year of 2013. Following the year of 2014 Article 285 has also been amended[56]. This is ongoing review as the government tries to bring the law into conformity with the European Convention. These amendments are designed to bring greater clarity to existing law, which in terms will bring Georgian legislation to the standards set by the Convention.

In 2014, new amendments were made to the Law on Data Protection which went into force. These amendments gave power to the Personal Data Inspector to inspect and monitor the data processing by law enforcement agencies. This includes inspecting the lawfulness of implementation of surveillance and interception during the covert surveillance activities

[55] Criminal Procedure Code. Parliament of Georgia. Legislative Herald of Georgia, Tbilisi, Georgia. Consolidated version. No. 1772, 2015

[56] Georgian Law on Personal Data Protection. Parliament of Georgia. Legislative Herald of Georgia Tbilisi, Georgia. No. 5669, 2011

envisaged by the Article 143.1 (a) of the Criminal Procedure Code. This covers telephone call, including eavesdropping and recording.

The modifications made in the Data Protection Law has much triggered amendments in the Criminal Procedure Code, the Law on Electronic Communications and the Law on Operational Investigative Activities.

Based on the amendments made in the Criminal Procedure Law on covert investigative activities, the process covert tapping and the phone conversation recording will be done under two-stage electronic system which needs a consent from law enforcement and the Personal Data Protection Inspector. This means that both the Inspector and law enforcement has now a direct access to the data of communication companies. The law enforcement officials will be given this right only after the court authorization. And they cannot start tapping personal data without electronic consent done by the Inspector. Granting so-called key in hands of the electronic communication companies instead of law enforcement is better as it would be hard to control the provider companies.

The necessary changes have also been introduced in the Law on Electronic Communications of Georgia. The law establishes legal and economic grounds for the pursuit of activities by means of electronic communications networks and facilities within the territory of Georgia, as well as incudes the principles for the development and regulation of the competitive environment in this sector. The Law also describes the functions of an independent national regulatory authority named as the Georgian National Communications Commission, which establishes the rights and obligations of natural persons and legal entities owning, using or providing services by means of electronic communications networks and facilities[57].

2014 amendments made to the Law on Electronic Communications, provides that in case if it is required, the electronic communications companies are responsible to have the technical ability in order to provide communications content and data from their networks to the monitoring systems of the authorized agencies. These companies are also required to inform the Personal Data Protection Inspector with respect to the identified data provided to the law enforcement agency[58].

[57] Georgian Law on Electronic Communications. Parliament of Georgia., 2011

[58] Georgian Law on Electronic Communications. Parliament of Georgia., 2011

3.3. Policy Recommendations

Since 2008, Georgia has taken significant steps in the development of cybersecurity. Nonetheless, addressing this issue successfully calls for implementation of a deliberate, consistent cyber policy, prioritized at the state level. Based on the amendment implemented in the law, the country is trying to catch up to its European partners. However, while the volume and sophistication of threats is rapidly growing, there are two main issues to achieve this. Firstly, the lack of awareness and secondly, the lack of resources. A major problem is related to the well-trained computer professionals. Developing a program to assist and train government officials is the best western practices. A series of seminars for professionals on advances topics like research on the deep web, anonymization and pro-active techniques to anticipate cybercrimes and cybercrime trends has a significant importance. Moreover, the government must implement and effective plan to replace government computers as needed and install only genuine software. The replacing and installing new hardware is time and cost related, however, this is inevitable to have the appropriate security systems.

In terms of policies and laws, Georgia should update the Cyber Security Strategy and Action plan with clear, specific and measurable objectives. And ongoing mechanism should be established to review its body of law regularly and methodically, to have the consultations with legal experts from partner countries, with Council of Europe and European Union and to submit its parliament proposed amendments that adapt changing technology and bring it even closer to European standards. It is also important to plan and implement a public awareness program to familiarize the public with cybercrime, with its threats and introduce preventive measures. Georgia can use best practices implemented in other countries. The public authorities should consult with media as well as with private sector to develop the best wats to reach various publics. All Georgian government employees should be delivered general computer courses focusing on key aspects of cybersecurity. Once public awareness program will have an impact, it is necessary to introduce a new cybercrime reporting mechanism modeled on other counties examples and adapted to Georgian needs.

In all these endeavors, it is important for the country to develop clear and measurable objectives. Georgia is actively cooperating with its partners and has learned how to gain knowledge from their experience and how to gain mutual benefit. Cybersecurity and cybercrime are global issues, therefore, fighting against this challenge required closer international cooperation and cooperation with like-minded countries.

4. LEGAL CONTEXT FOR CYBER VOLUNTEERING: REGULATORY APPROACHES OF GEORGIA AND ESTONIA

4.1. General Regulatory Framework for Volunteering

“Volunteering is the commitment of time and energy for the benefit of society and the community, the environment or individuals outside one's immediate family. It is undertaken freely and by choice, without concern for financial gain.”[59] Volunteering is a matter of choice and is a legitimate way in which citizens can participate in the activities of their community. It is an activity performed in the not-for-profit sector only and is not a substitute for paid work[60].

The Universal Declaration on Volunteering is the framework for International Association of Volunteer Work (IAVE) which exists to promote, strengthen and celebrate volunteering in all the myriad ways it happens throughout the world with more than 70 countries involved. It is a connective tissue of a global network of leaders of volunteering, NGOs, businesses and volunteer centers that share a belief in the power of volunteers to make a significant strategic contribution to resolving the world’s most pressing problems advocacy efforts which was first issued in 1990 during the World Volunteer Conference in Paris. This Declaration supports the “right of every woman, man and child to associate freely and to volunteer regardless of their cultural and ethnic origin, religion, age, gender, and physical, social or economic condition”[61]. “Volunteering is a fundamental building block of civil society. It brings to life the noblest aspirations of humankind – the pursuit of peace, freedom, opportunity, safety, and justice for all people”[62]. In the modern world with the globalization and rapid changes, the world is becoming independent and more complex. “Volunteering – either through individual or group

[59] Fingal Volunteer Centre, Definition & Principles of Volunteering, www.volunteerfingal.ie/index.php/organisations/articles-for-organisations/165-definition-a-principles-of-volunteering.html (15.02. 2017), 2017

[60] International Association of Volunteer Effort, www.iave.org/about-iave/ (23.04 2017), 2017

[61] Universal Declaration on Volunteering. International Association for Volunteer Effort. The Netherlands. www.fcsh.unl.pt/ensino/voluntariado/DeclaraoUniversaldoVoluntariadodeJaneirode2001.pdf (20.11.2017), 2001

[62] *Ibid.*

action – is a way in which human values of community, caring, and serving can be sustained and strengthened"[63]. Individuals can freely exercise their rights and responsibilities as members of communities[64].

Volunteerism has become an essential element of all societies in today's world. It turns into practical, effective action the declaration of the United Nations that "We, the People" have the power to change the world. The Declaration supports "the right of every human, to associate freely and to volunteer regardless of their gender, religion, cultural, ethnic origin, age, and physical, social or economic condition"[65]. All human has the right to offer their time, talent and energy to others, without expectation of financial reward.

Volunteerism concept in EU legislation is enshrined by the actions such as free will of the individual, development through non-profit or non-governmental organizations, who have no professional character and performed for a community or a third party. It is noteworthy that in most of the EU Member States' legislations, the volunteer concept is not defined or regulated. Legal definitions make a clear distinction of volunteering from employment. For instance, in the Romanian law we can find the following wording: "volunteer activities are other than labor relationships and the relationship arising between employer and remunerated employees[66]."
As it provided by the Italian law, the role of a volunteer is incompatible with all kinds of employer to employee relationship where income is received from the organization. Moreover, according to Belgium law, a volunteer cannot perform the same activity as an employee and as a volunteer for the same organization and employer. A person can volunteer within their own organization provided that a clear distinction is made between the activity they perform as paid staff, and the activity they perform as a volunteer. Netherlands where some volunteers get benefits like free access to festivals, etc.[67]

[63] *Ibid.*

[64] Basilaia, M. Volunteers and Cyber Security: Options for Georgia. Tallinn: Tallinn University of Technology, 2012, p 10

[65] Universal Declaration on Volunteering. International Association for Volunteer Effort. The Netherlands. www.fcsh.unl.pt/ensino/voluntariado/DeclaraoUniversaldoVoluntariadodeJaneirode2001.pdf (20.11.2017), 2001

[66] Wernberg-Tougaard, C. IT-Security Beyond Borders — an Assessment of Trust Levels Across Europe. Unisys EMEA, 2007, p 23

[67] Hadzi-Miceva, K. Comparative Analysis of European Legal Systems and Practices Regarding Volunteering. Paris: OECD Publications, 2006, p 1-12

Various nature of volunteering leads us to above mentioned fact, that there is no uniform way of regulating. Three kay distinctions can be pointed out, among member states, by categorizing the regulatory framework for volunteers. Those are: firstly, member states, where legal framework regarding volunteering is in place. Such as for Belgium, Cyprus, Czech Republic, Hungary, Latvia, Luxembourg, Malta, Poland, Portugal and Spain[68]. Secondly, member states, where is no legal framework or specific laws for volunteering, but they are regulated by or implicit within other existing general laws, such as for Austria, Denmark, Estonia, Finland, France, Germany, Greece, Ireland, Lithuania, Netherlands, Slovakia, Sweden and the UK. And finally, member States who are in the process of developing a legal framework for volunteering, as Bulgaria and Slovenia. Luxembourg, Malta, Poland, Portugal, Romania and Spain have specifically implemented laws which apply to volunteers. These laws are the main legal frameworks for regulating volunteerism. Notwithstanding that some laws exist and are in place, there is still limited information to determine whether legal framework has made any positive influence from the perspective of individual or voluntary organizations.

In many countries, legal framework is used only to determine the legal definition and status of volunteers to protect and support them. It is noteworthy that clarification of their status and definition is important when making the distinction of paid employment and volunteering. For example, in Hungary, volunteers' status was not regulated until 2005 and organizations which had full time volunteers used to pay them money. There are number of countries where there is no legal framework in place. Volunteers and volunteering are implicit within and regulated by general laws. It is hard to state general conclusion why there is no such laws which regulates volunteers. For example: in Sweden, up to now regulating volunteers and volunteering organizations and an attempt to formalize it in the law or in legal frameworks is abandoned[69]. This is because that they are giving a priority of freedom and autonomy of this sector. The legal framework and legal aspect of volunteering is currently under development in a relatively small number of countries of the European Union. This is due to the urgent need to provide a legal status for volunteers and regulate the operation of organizations engaged in volunteer activities.

The main reason for drawing a clear line between a volunteer and a paid member staff is to define and regulate many other issues surrounding it, for example, tax benefits, health and

[68] *Ibid.,* 10

[69] Koops, B.j. The Internet and its Opportunities for Cybercrime – Transnational Criminology Manual, Vol. 1, 2017, p 744-745

safety, insurance, welfare benefits etc.[70] In approximately half of all Member States there is no legal framework in place for volunteers and therefore no specified legal provisions on their rights and responsibilities[71]. Though there is no legal status for volunteers in many countries, volunteers are subject to the same rules as people in paid employment.[72] Generally, the level of volunteering depends on many aspects. For example, economic and political situation, the stage of development, culture of volunteering, and the labor markets. Legal framework becomes important when it creates difficulties and impedes volunteering. Defining of voluntary service on national level and giving volunteers legal status can assume as important aspect and one step forward in any countries legislation. Also, it's noteworthy to eliminate and reduce any obstacles which prevents humans from engaging in volunteer actions directly or indirectly.
There is a long list of benefits society and communities can get from volunteering. Citizens are more engaged in social life. Thus, the sense of responsibility and mutual care becomes more and more important for citizens which can result in dealing effectively with many social issues. Volunteering can also increase skills and self-confidence in the volunteers themselves and enables the elderly to remain engaged to contribute to the common good[73].

The legal aspect of volunteering is very important, because many laws like labor, tax etc. affect it both directly and indirectly. Problems that can arise in the legal field are among others liability issues, rights and obligations, taxation and so on. National law shall deal with the relationship of volunteering and employment by providing a comprehensive legal act to clearly draw a line between these two. The emptiness in legislation concerning the legal definition of volunteering may result in the treatment of volunteers as paid employees. The law should be aiming to replace the impediments to volunteering with the incentives. Some issues can arise in regards of regulating volunteering. Considering that volunteering can take many forms, from spontaneous initiatives to organized formal programs, community based organizations to international ones, it may prove very difficult to regulate all forms of volunteering. Experts agree that legislators should "ensure that laws with specific purposes do not restrict opportunities for the enhancement of an enabling volunteer environment.[74]" Otherwise the

[70] *Ibid.,* 745

[71] Gyenes, R. A Voluntary Cybersecurity Framework Is Unworkable- Government Must Crack the Whip. - Pittsburgh journal of technology law, Vol. 14, No. 2, 2014, p 103- 293

[72] *Ibid.,* 119

[73] Klimburg, A. The new Cyber threat: Mobilizing Cyber Power. Journal Survival, 2011, p 54-55

[74] Kostyuk, N. International and Domestic Challenges to Comprehensive National Cybersecurity. Journal of Strategic Security, Vol. 7, No. 1, 2014, p 1-17

whole concept will be distorted. By the virtue of this, it is important that governments and CSOs clearly set how they want to deal with legal aspect of volunteering and avoid controversies during legislative drafting. The main idea of volunteering, which is generally considered an altruistic activity, is to provide services to persons without any mercantile intentions. So, national laws shall be aimed to facilitate such activities by providing protection and promotion rather than controlling it. Over-regulation may result in decrease of morale and volunteer spirit.[75] Based on its social, cultural, economic conditions, countries should decide and have some leverage how to regulate volunteering. Governments should evaluate their legal systems and identify how local laws affect volunteering, to determine how legal changes can best harmonies with local needs.

4.2. Volunteerism in Georgia

In case of Georgia, the phenomena of cyber volunteerism are relatively new. There is nothing mentioned in the legislation of Georgia with respect to the cyber volunteers. The law does not recognize the actions of the cyber volunteers, as such. Despite this, the facts provided in this master thesis proves that the cyber volunteers do examine their actions in Georgia illegally. Ratification of norms that controls the conduct is one thing and make jurisdiction over the conduct which can be committed from any spot of the world is another. From the perspective of government, it can be the dilemma on how to regulate this, who to blame in violent conduct etc. From the perspective of hackers, who have good knowledge of IT sphere, revealing their knowledge and power can be fatal, because they can be caught and be imprisoned. This master thesis recommends that such hackers should be used in favor of government, and not to put them in jail. Government should implement the regulatory frameworks, which will give possibilities to hackers to disclose themselves and help government to defense their country and to improve cyber infrastructure.

Non-governmental organizations such as Helping Hand and the Civil Society Institute have conducted studies in Georgia with respect to volunteerism. The outcome of the studies indicates that in Georgian society the concept of volunteerism has not taken root yet. Moreover, surveys taken by the Caucasus Research Recourse Center (CRRC) showed a mismatch between the actions taken regarding the volunteerism and the attitude within the society. According to the CRRC-Georgians Caucasus Barometer survey which was contacted in 2013, “68% of

[75] Wiener, N. The Human Use of Human Beings. – Free Association Books, Vol. 1, No. 2,1989, p 61-62

Georgians find it important for a good citizen to do volunteer work"[76]. Whereas, in contrast, "only 19% of Georgians reported volunteering during the past six months before the survey was carried out in fall of 2013"[77]. These numbers illustrate a clear gap existing between actions and attitudes. Interestingly, while the share of the population highlighting the importance of volunteerism for good citizenship increased between 2011 and 2012, the share of Georgians who volunteered did not change much. Thus, according to these numbers, volunteering in Georgia is not considered as important as some other traditions. For instance, traditions such as voting in the elections or supporting people in need. However, notwithstanding to the existing mismatch, the level of volunteerism is not significantly low if we compare Georgia to some European countries. In 2010, the studies with respect to volunteerism in the European Union was conducted by the British consultancy called GHK Holdings Limited. Based on the study, only few European countries showed the highest rates of volunteerism. These countries were Austria, Netherlands, the UK and Sweden with 40% of volunteering rates. This number is high comparing to Georgia with 10-19% of rate and other European states such as Italy and Greece where is volunteering rate is the lowest, with only 10%[78].

To set the prospects for improving the level of volunteerism in Georgia, it is important to determine the main trends to volunteer in the country. Identifying these trends will allow non-governmental organizations, policy makers and social entrepreneurs to know where to direct their programs aiming to increase the volunteerism. According to the 2013 Caucasus Barometer survey there are some differences between the socio-demographic groups. For instance, "the elderly aged 56 and older are slightly less active (14% reported volunteering) than 18-35 and 36-55-year-old (20% and 22%, respectively)"[79]. This low rate is logical as the activity level of the aged people is generally low. The same survey showed the difference between the gender. Males are tending to be involved in volunteering activities in Georgia more than females "(25% and 14%, respectively) and inhabitants of rural areas are slightly more actively engaged in volunteering (24%) than inhabitants of the capital (14%) and other

[76] Zubashvili, N. CRRC-Georgia: What we know about volunteering in Georgia. - Caucasus Research Resource Centers Georgia, Issue 6, 2015
www.investor.ge/article_2015_6.php?art=8 (18.11.2017)

[77] Zubashvili, N. CRRC-Georgia: What we know about volunteering in Georgia. - Caucasus Research Resource Centers Georgia, Issue 6, 2015
www.investor.ge/article_2015_6.php?art=8 (18.11.2017)

[78] *Ibid.*

[79] *Ibid.*

urban areas (15%)"[80]. To compare these numbers with the European Union countries, GHK study shows that the level of education has a significant influence on the level of volunteering. In contrast, the level of education does not have any impact with respect to the involvement in volunteering in case of Georgia. The education factor, age difference or gender does not have a direct impact on the attitudes towards the volunteering. However, the settlement type is a differentiating factor and according to the 60% of inhabitants of Tbilisi volunteerism is important aspect for defining a good citizen. The numbers change in other urban or rural places where the number increases up to 68-72%. These rated are striking when it comes to age groups within a settlement type. During the 2015 floods which took place in Tbilisi, most of the volunteers were young people. However, the were the least likely age-settlement group considering that the volunteerism was an important aspect for a good citizen[81].

The participation of young people as volunteers following the flood in Tbilisi showed that the country has a potential to increase the overall level of volunteering. Therefore, non-governmental organizations, including policy makers and social entrepreneurs should consider the ways to work off the existing attitude of volunteerism which was embodies by the cleanup efforts and supportive actions towards volunteerism in the country. In 2013 survey provided by CRRC's Caucasus Barometer, proves that there is a rise of volunteerism in the country. Moreover, during the years 2013-2015 minor positive changes have been observed with respect to the approaches towards volunteerism amongst all socio-demographic groups[82].

Importance of volunteers for a country reveals that volunteerism saves internal recourses. Volunteers are helping the country to strengthen their ability of defending itself and taking no money for the service. And what volunteers gain from such free will is that they develop their skills, get trainings for free, thus, becoming more sophisticated. Even though, a slight discrepancy remains between the reported levels of volunteering compared and the citizen's attitudes towards it, the present fluctuations may indicate a trend that volunteering may become more common in Georgia. Actions such as volunteering could inspire and serve others as an example to do the same.[83]

[80] *Ibid.*

[81] *Ibid.*

[82] Caucasus research resource group, Volunteerism in Georgia Between 2013-2015: Attitudes and Practice, 2016 www.crrc-caucasus.blogspot.com/2016/03/volunteerism-in-georgia-between-2013.html (20.03.2017).

[83] Yar, M. The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. - European Journal of Criminology, Vol. 2, 2005, p 407-427

4.3. The Role of Georgian Cyber Security Bureau and Cooperation on International and National Levels

The provisions regarding the cyber security is difficult to achieve only on a national level. The best way is if the implementation process is coordinates as on international as well as on national level. It is important for the country to develop the relations on multinational and bilateral level. This relations entail support from European and North Atlantic Treaty Organizations to discharge the obligations which are useful to increase the level of the cyber security and the cyber security provision itself. The Ministry of Defense (MoD) should encourage local Computer Security Incident Response Teams (CSIRTs) to establish cooperation with the other countries' CSIRTs. This includes to introduce and implement new standards, different approaches and principles on local level in compliance with Georgian legislation. The establishment of a close international cooperation in respect of legislation is also needed, as the nature of cyber space is very dynamic and motives of attackers are often changing, and most frequently it is difficult to define which legal actions are to be taken for the specific case[84].

Joint support, interagency collaboration and active coordination with both state bodies and private sector is a strategic part of cyber security provision. Based on the world practice, agencies cannot succeed in many facets of securing cyber space if they work on their own. Reinforcement of close cooperation in cyber security field facilitates information sharing, application of international experience and best practice. Cooperation on multinational level in cyber security will help to develop and secure the information and technology field. The bureau mentioned above was actively working on raising the awareness in cyber security. Georgian national guard jointly with the J-3 operational planning department has implemented and developed a new project which aims the formation of the National Guard deputy base of cyber security. The multinational cooperation has a significant meaning as this project was launched which Georgia's partner countries such as Estonia, Latvia, Lithuania and Ukraine.

Georgian Cyber Security Bureau was established based on the law of Georgia on "information security" and on "approval of the Decree on the establishment of LEPL – Cyber Security Bureau", decree no. 8, issued by Minister of Defense of Georgia in February 6, 2014. The

[84] Friis, k., Ringsmose, J. Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives, Routledge, 2016, p 1-130

Cyber Security Bureau elaborates information security policy in the defense field, defines emerging and potential risks and challenges in cyber space, and methods for its timely eradication and prevention. Furthermore, bureau strives to refine appropriate legislative framework and harmonize them with international norms. At the same time, Bureau participates in development of Cyber Security Strategy and accompanied Action Plan. Security of information and communication technologies in Georgian Defense field aims to rapidly identification of threats and risks, provision of responsive actions on computer incidents and preventive measures. These activities are carried out in a standardized way by the Computer Security Incident Response Team, work cycle of which is elaborated based on world's best practice and includes the essential actions to promote the timely identification and elimination of computer incidents.

In April 2015, Georgian Cyber Security Bureau participated in the “Black Sea and Caspian Sea Security Symposium" where the main topic was regarding the “Cyber Security - Global Security"[85]. The symposium was organized by the European Command of the Unites States. Heads of the military intelligence agencies take a part in this annual event from various countries from the region of Black and Caspian Sea. Shortly after this event, the cyber security bureau participated in the annual meeting attended by the executives in overseas-accredited diplomatic missions in Georgia. The attendees have been informed about the usage of the elements of cyber in post-Soviet conflicts. In addition, the importance of cyber security and possible self-defense mechanisms was discussed during the meeting. The cooperation on the international level has a significant meaning to achieve effective developments in the field of cyber security and cyber defense. When discussing the cooperation on international level in cyber security, it is worth mentioning the meeting of the NATO-Georgia Commission which took a place in the NATO headquarters, in Brussels. During the meeting, the parties discussed the possibility for the bureau to be involved in the Smart Defense projects introduced by the NATO. These projects entail education and training program in the field of cyber defense, exchange of information on multinational level with respect to the malicious software, etc. The admission for Georgia to participate in NATO cyber projects will be possible when the country will fully complete the NATO standard procedures. To further develop the international cooperation on cyber security, the meeting was held between the Georgian defense attaches

[85] Zekos, G. Cyberspace and Globalization, Legal problems in cyberspace. - Law, Social Justice & Global Development Journal, 2002, p 2-29

who were stationed abroad. The focus of the meeting was devoted on the existing threats in cyber space and the possibilities were discussed on how to fight against it. For cybersecurity provision purposes, it is important for Georgia to identify the strategic partners and the potential enemies. The same identification procedures should be conducted with respect to the organizations which present a threat for Georgia's national cyber security. And cooperation with the strategic partners will strengthen and benefit the country's national security.

The multinational cooperation and participating in the conferences is important for Georgia as it helps to develop the level of cyber security in the country. Sharing of knowledge and experienced from other countries helps to implement more effective actions in this field.

4.4 Main Priorities of Cyber Security Policy and Analyzing Cyber Attacks on Georgia

Cyber Security policy of Georgia includes some of the compelling priorities in the of which is necessary to meet the objectives set out in the document. One of the core priorities of the policy is defining the main strategy in terms of the cyber security provision. The Policy provides an overview of the main principles which can possibly create the safe infrastructure and includes the strategies to have a safe protection of the information systems and network in the country's defense sector. The Policy also provides the collaborative engagements from local structures to facilitate the MoD in securing its critical infrastructure[86]. The second important priority set out in the Policy is regarding the protection of the information systems of Georgian Armed Forces. To develop an effective method and means for intelligence and radio digital fighting in order to avoid potential cyber-attacks. As the cyber-attacks has a significant growth, the MoD of Georgia stresses on creation of a secured information environment, which is the precondition for stable functioning of ICT infrastructure. Due to the dynamic nature of cyber space, there is now a need to consider all cyber security related issues within the framework of Cyber Security Policy highlighting an integrated vision and coordinated strategy for implementation.

Russia holds a broad concept of information warfare, this includes intelligence, counterintelligence, degradation of information systems and propaganda. In today's word

[86] Thoron, L. Public Attitudes in Georgia. Tbilisi: National Democratic Institute, 2015, p 1-10

computers are among the many other existing powerful tools of information warfare. In August 2008 Russia carried out combined cyber and kinetic attack along with land, sea and air attacks, because of which important part of Georgia's critical infrastructure was damaged and the country fell into informational vacuum. In 2008, for Georgia has experienced the first ever combined kinetic and cyber attach. Thus, it was one of the first practical test of this doctrine. This incident of continuous cyber-attacks conducted by Russia for 2008-2014 years had a major and direct effect on Georgia's government and private sectors. These cyber-attacks were conducted from Russia as well as from its occupied Georgian territories, such as Sokhumi, Abkhazia located in south-western flank of the Caucasus Mountains.

According to the research conducted by the American information security company - "Fire Eye", during the years 2008-2014 Russia carried out continuous attacks on the Ministry Internal Affairs and the Foreign Affairs webpages, including the pages of the president, the parliament, news agencies and banks and various NGOs[87]. One year later after 2008 war, on August 6-7, 2009, once again the attack was conducted by Russian hackers on the popular Georgian social network, that was stipulated by the political opinions of a Georgian blogger "Sokhumi". Shortly, on August 7 the blogger's web page which included the blog regarding the information on the anniversary of the August was blocked. Thus, it was clear that Russian special services were behind the attack. The attack on the web pages was brought down and was so well organized that it rules out the possibility of it being carried out by individual hackers. Moreover, the hackers did not only attack Georgian government's official Web sites, but they have brought down the Russian newspaper called Skandaly.ru. The reason was that the newspaper expressed pro-Georgian opinion. Thus, together with the external target, they have committed internal attack.

As the below mentioned facts confirm, one of the main targets of Russian hackers are web pages and other resources that protect Georgia's state interests on the net. In addition, the cyber-attacks conducted by Russia serve the purpose of obtaining information regarding Georgia's external relations with the US, the EU and NATO and plans via the means of cyber espionage. The attacks against Georgia's Internet infrastructure began earlier than the 2008 war with the well-coordinated barrages of millions of requests which is known as distributed denial of

[87] Ministry of Defense of Georgia, Report on Cyber Security, 2015, p 4-43

service, or DDoS, attacks. Based on the government data, in 2015, Russia's presence in the Georgian cyberspace was not noticeable and no attempts of access were observed, however:
On May 21-25 - a massive Distributed Denial of Service (DDoS) attack was carried out on Georgian financial organizations. Total of 300,000 unique IP addresses from over 160 countries participated in the attack[88]. According to the scale and the quality of this attack, and taking into consideration the geopolitical interest in the region by Russian side, there is a ground for the assumption that the hacker group responsible was once again backed by the Russian government. Since January 2015 to this day multiple cyber-attacks were conducted by Islamic hacker groups, for instance, on January 10, a cyber-attack was carried out on the Georgian branch of the French company "Carrefour" for which Middle East Cyber Army (MECA) claimed the responsibility. This attack was conducted at the same time when the massive cyber-attacks were conducted on French companies and their branches/offices around the globe, among which was the Georgian branch of Carrefour. This is important fact which should be discussed as a precedent for Georgia which might again take place in the future, and such incidents might become more common. Following the January 10 incident, in couple of days on January 19, the Office of the State Minister of Georgia for Diaspora Issues came under a cyber-attack. On February 2, a massive cyber-attack was carried out on email accounts by a new computer virus which was distributed online. The virus sent emails in different languages including in Georgian. The virus gave the users 96 hours to deposit a specific amount of money, otherwise it threatened the users to permanently delete their files. On February 5, another cyber-attack was carried out on the official website of the Ministry of Foreign Affairs. The attack led the Ministry to create a new website. The source of this cyber-attack remains unknown. On April 16, Islamic hacker group "Al Muhajir" carried out an attack on the "Georgian Judges Association" website. On July 6, ISIS hackers conducted cyber-attacks on the Office of the State Minister of Georgia on European and Euro-Atlantic Integration official website.

According to the official statistical data provided by the Ministry of Internal Affairs, cybercrime is increasing rapidly on a daily basis, whereas the percentage of the solved cyber-crimes has majorly decreased. Namely, the number of cybercrimes identified by the Ministry as of January - August 2015 has increased by 11.11% compared to 2014. As for cybercrime

[88] Tsatsanashvili, M. *"Information Law"*. Tbilisi: Tbilisi Publishing Limited, 2004, p 1-12

solution, the 2014 solution index made up 59.26, whereas for 2015 January through March it is 34.44%.[89]In addition to the various cyber-attacks discussed above, several other attacks were carried out against various Georgian organizations and agencies. According to the information provided by zona-h, Georgian cyberspace was affected by 489 incidents of unauthorized access over the period of January through March[90]. This number might not be too high for bigger countries such as the United States, United Kingdom, or China. However, for Georgia, the detected number of illegal access causes certain concern. The number of the cyber incident takes place quite often.

Pilot project has been elaborated in coordination with National Guard and J-3 Operations Planning Department, based on the best practice of partner countries such as UK, Estonia, Latvia, Lithuania and Ukraine, which is aims the establishment of Cyber Reserve based on the reserve of National Guard.[91] The mission of the project entails the provision of cyber and information operations in cyberspace based on state interest during peaceful, warfare and during the emergency situations. The purpose of the project is attracting and retaining high qualified specialists from business sector to improve additional capabilities. The mechanism is a gradual, voluntary recruitment of the reservists working in the field of IT at critical service providers, training and action scheme development in a crisis. There are state benefits such as for instance, building and strengthening additional capabilities for the provision of cyber defense and information operations, integrating high qualified staff in the field of cyber security with minimal cost of financial and human resources.

4.5. Regulatory Framework for Volunteerism in Estonia: Comparison with Georgian Regulatory Framework

A variety of laws affect volunteering activities in Estonia. There are two key national documents in Estonia with respect to civic initiatives and volunteering. Estonian Civil Society concept was initiated in 1999 with the financial support from the United Nations Development Programme (UNDP). The mission and the goals of the civil society is written down in a strategy

[89] Lehto, M., Neittaanmäki, P. Cyber Security: Analytics, Technology and Automation. Springe: Springe Punishing, 2015, p 12-19

[90] Jayakumar, Sh. State, Society and National Security: Challenges and Opportunities in the 21st Century. Singapore: World Scientific Publishing, 2016, p 1-16

[91] Wernberg-Tougaard, C. IT-Security Beyond Borders — an Assessment of Trust Levels Across Europe. Unisys EMEA, 2007, p 12-14

document which is known as Estonian Civil Society Development Concept (CSDC) – EKAK from its Estonian acronym. CSDC forms the basis of the national strategy for the civil society development, the document also defines the mutually complementing roles of the public authorities and civic initiative, including the core principles of the cooperation of these two and the main mechanisms and the priorities. One of the purposes is to prove that there is a mutual understanding between the government and non-profit organizations about co-operation between the two parties. The CSDC was developed in 2002, when the Estonian Parliament adopted the CSDC. It was adopted as a basis for co-operation with the Third sector. The CSDC stresses on the role of voluntary activity in the development of civil society As it is promoted in the concept, the active participation is an important form of social engagement in the voluntary associations. This has a positive impact on democracy as well as on individual's personal development. It specifies the roles and principles by which public authorities and civic initiatives should develop and implement public policies. The implementation of the Concept is mainly overseen by the representatives from the different ministries and the non-governmental organizations (NGO). Every year, committee submits a report to the government and to the public. And every second year there is a public discussion held in the Parliament where different issues are being addressed. Thus, the Concept outlines, among others, that its goal is to "support the idea of voluntary action, being one of the essential features in acting as a citizen… Citizen action, self-initiative, and voluntary participation in public life are an integral part of the democratic society has a major importance and meaning. The authorities support it by creating a favorable legislative environment, informing the public about their work, involving citizens and their associations in the planning and implementation of relevant decision."[92]

To implement the objectives which were included in the Estonian Civil Society Development Concept, the Ministry of Interior with its strategic partners and with the involvement of the public sector has prepared a new Civil Society Development Plan which came into force in 2015. The Estonian Government has adopted the development plan, which aims the promotion of civil society from 2015 including 2020. Two main priorities are provided in the plan. First one regarding some socially active residents and the second one about acting capabilities of citizens' associations with respect to ensuring the sufficient possibilities for the citizens'

[92] National Report on Volunteering in the European Union, Country Report Estonia, www.ec.europa.eu/citizenship/pdf/national_report_ee_en.pdf (19.03.2017), p 3-33

associations to achieve the goals. One of the main goals of the development plan is to establish the goal for the citizens' associations to participate in forming a policy as a natural cooperation. Also, it aims to increase the influence of citizens' associations in the process of dealing with social problems and improvement of well-being of people through social innovation, social entrepreneurship etc. in public service. The activities related to the development plan is financed by the state budget together with the external resources. In addition, private and the third sector financial sources are used as a finance source. The development plan of the field is being executed based on the implementation plan prepared for the years 2015–2018, and it is being updated annually for the upcoming four years.[93]

Estonia and Georgia, these are countries which became victims of cyber-attacks in different periods of time. Both have experienced to take defensive measures against such conducts. Following the Russian aggression, Estonia has established the Estonian defense league, which will serve as a commander of the defense forces during wartime. This was a good example for Georgia to create a similar defense structure. In 2008, after Russian aggression it has been revealed that country wasn't ready for such attack. The event of 2008 became turning point to reinforce the country's cyberspace defense. It's important that Georgia identifies who is its strategic partner for it. Estonian experience became the example for the country and there was created Georgian cyber security bureau. Similar organization as Estonian cyber defense unit, with some differences. The difference between these two organizations is volunteerism. In Estonian defense unit, people can become members voluntarily. Those who desire to defend country and have an ambition to became more developed skills can become volunteers. Although, it is important that the potential members have a good IT knowledge. Unlike from Estonia, in Georgian cyber security bureau, there is no such kind of opportunity to volunteerism, this is rather an official job.

Estonian public and private sectors are collaborating with each other more, than Georgian ones. Representatives of private sector, the organizations which are orientated on IT field are helping government to strengthen cyber defense. They cooperate with governmental sector and supply them with skillful people in the IT sector. The cooperation between private and governmental

[93] Ottis, R. (2011) Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability, www.ccdcoe.org/multimedia/theoretical-model-creating-nation-state-level-offensive-cyber-capability.html (18.12.2017), 2011, p 1-7

sector should be improved in Georgia. If the government would give the possibility to private sector to finance more projects in the field of IT, it would rapidly improve the overall level IT level. It is stated in this master thesis that in Georgia it can be seen slowly but steady progress regarding the above mentioned.

The articles regulating cybercrime were added to Estonian legislation in 1997. Estonia ratified the Council of Europe Cybercrime Convention on May 12, 2003 which contains the articles with respect to the computer sabotage, article 208 Regarding the damaging of connection to computer network, article 217 about spreading of computer viruses and article 284 regarding the unlawful use of computer, computer system or computer network. Punishment regarding such conducts is subject to imprisonment approximately from 1 to 3 years[94]. Estonia is much more sophisticated and developed in the field of cyber security. Estonia's legislation framework to this regard it much more developed. This field is starting to develop in Georgia as well. The cooperation between these two countries in the field of cyber security, and sharing Estonia's experience helps Georgia to move forward in cyber security and expand human resources.

Unlike Estonia, cyber volunteer conduct is not regulated in Georgia, by any means. The threats can be significant for the country. It is hard to distinguish where does the state capability ends and independent nationalistic group hacker/volunteers begin.

4.6. Main Public Body Responsible for Volunteering and Role of Estonian Defense League in Cyber Security

In Estonia, it is the Ministry of Interior responsible for analyzing, planning and coordinating active community development and co-operation between the state and the NGOs. The Joint Committee of the Government and NGOs was formed in 2003 and reformed in 2007 to include higher state representatives[95]. The Committee oversees the implementation of the Civil Society Development Concept, and it is the Minister of the Interior which oversees the committee. The committee consists of about 20 members, including bigger umbrella organizations. However, not only the Ministry of Interior is primarily involved in the development policy agenda, but

[94] Lehto, M., Neittaanmäki, P. Cyber Security: Analytics, Technology and Automation. Springe: Springe Punishing, 2015, p 17

[95] Choucri, N., Madnick, S., Ferwerda, J. Institutional Foundations for Cyber Security: Current Responses and New Challenges. Cambridge: Massachusetts Institute of Technology, 2013, p 5-13

there are number of Ministries taking active part in this, such as, the Ministry of Justice which is volunteering in probation services, the regulations screening volunteers working with children, the Ministry of Environment, volunteering in the environmental field, the Ministry of Foreign Affairs, volunteering abroad ant etc. In addition, many voluntary organizations actively collaborate with local governments. For instance, City Government of Parnu has been involved in the international co-operation project of activating elderly people through volunteering.

The Estonian Defense League which is a part of the Estonian Defense forces has a Cyber Unit (EDL CU) which serves as a voluntary organization aiming to protecting Estonian cyberspace. The Unit is being established as a structural unit of the Estonian Defense League. The status of the Unit derives from the legal acts defining the status of the latter. One of the main missions of Estonian Cyber Unit is to protect country's high-tech way of life. This includes the information frustration protection together with supporting national defense broader objectives. The Cyber Unit includes a core group of highly professional and trained specialists in the key cyber security positions in national critical infrastructure, patriotic individuals with IT skills, including youth who are ready to contribute to cyber security, and specialists in other fields that concern cyber security who promote the cyber security objectives in the population. EDL CU focuses on a development of cooperation between the highly qualified volunteers working in the IT field as well as improving the cyber security level for critical information infrastructure by providing training and creating a network that facilitates public- private partnership and enhances readiness in operating during a crisis situation, education and training in information security, participation in international cyber security training events.

The Estonian Defense League is an innovative model for the involvement of volunteers in national cyber defense. The League possesses arms, engages in military exercises and fulfils the tasks prescribed by the National Defense League Act. The Estonian Defense League has a long history in the Estonian independence and statehood. It was established in November 11, 1918 as a self-defense organization which was followed after the declaration of independence from Soviet Russia. Thus, it was founded as an armed voluntary defense organization to ensure the public order. By nature, the Estonian Defense League is a legal person in public law whose legal structure is defined by law and by the secondary legal acts. Thus, it is a legal entity governed by public law. The Estonian Defense League is an organization outlying of any political party. This means that all kinds of political activities of political parties and other political associations and their representatives are prohibited in the Estonian Defense League. One of the main goals of the Estonian Defense League is to enhance, by relying on free will and self-initiative, the nation's readiness to defend the independence of Estonia and its constitutional order. The activities of the Estonian Defense League are provided by the Estonian Defense League Act, the Statutes, which prescribe internal organization of the Estonian Defense League more precisely. The procedural rules which prescribe relations of active members of the Estonian Defense League to the codes of conduct of the Defense Forces, rules of conduct and internal administration procedure. The League enrolls 16,000 members[96].The procedure regarding the membership and withdrawal from the Estonian Defense League is on a voluntary basis and is subject to the procedure provided by the Statutes of the Estonian Defense League. Members of the Estonian Defense League represent honorary members who may be Estonian citizen or foreigner who has proven distinguished favors before the Estonian defense League. Members of the League can also become juniors as well as the supporters of the League. A supporter may be a citizen of Estonia or a foreign country who acknowledges the goals of the Estonian Defense League and contributes to achieving these goals by virtue of their activities. Estonian citizen of 7 - 18 years old are also given a chance to become a member of the League. For this, they should acknowledge the goals of the Estonian Defense League.

As it was already discussed in this research, purpose of the Estonian Defense League is to prepare population to defend the independence of Estonia and its constitutional order by relying on free will and self- initiative. This principal purpose also applied to the Cyber Defense Unit. The core objectives of the Cyber Defense Unit center are to develop a cooperation which will serve as a response during the crisis. This is reached by strengthening cooperation among qualified volunteer IT specialists as well as by the expertise of public and private sectors to act in crisis. Improving the security of critical information infrastructure. This can be reached by raising the level of security of critical information infrastructure. Promoting awareness, including the education and training. This entails an actively participating in cyber security training networks, as on local level as well as on international one[97].

[96] Cardash, S., Cilluffo, F., Ottis, R. Estonia's Cyber Defense League: A Model for the United States. Studies in Conflict & Terrorism, 2013, p 777-787

[97] Friis, k., Ringsmose, J. Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives. Abingdon: Routledge, 2016, p 5-23

During the cyber-attack campaign, the Estonian CERT was assisted by an informal network of volunteer cyber security experts. This provided much needed additional capabilities, such as increased situational awareness, analysis capability, quick sharing of defensive techniques between targeted entities, as well as an extended network of direct contacts to international partners[98]. The roots of this informal group derive from the late 1990ies, when Estonia was adopting a national ID card system. A later development was the formalization of this loose cooperation into the Cyber Defense League (CDL) in 2009. The Defense League is a volunteer national defense organization in the military chain of command. The CDL is part of the Defense League and unites cyber security specialists who are willing to contribute their time and skills for the protection of the high-tech way of life in Estonia, especially assisting the defense of critical information infrastructure. It is a defensive organization, not designed to harass political adversaries in cyber-attack campaigns. In January 2011, the CDL was reorganized into the Cyber Defense Unit of the defense League, but the CDL name is still widely used[99]. CDL's key activities include organizing training and awareness events, as well as cyber defense exercises. The CDL took a part in the Baltic Cyber Shield exercise in 2010 which was held by Cooperative Cyber Defense Center of Excellence together with the US-let International Cyber Defense Workshop including various national exercises. The CDL is a good example of managing in a productive manner the expertise and enthusiasm of motivated cyber security specialists[100].

4.8. Recommendations for Georgia

The aim of this chapter was to get over the deficit of human resources in Georgian IT sector and find the solutions to develop defensive cyber capabilities of the country. The solutions with respect to the volunteers is cost-effective and possible to implement immediately. The chapter focused on volunteerism bringing example from Estonia. After examining of Estonian example, formation and analysis of the current situation, the author concluded that the best option for Georgia is to pursue the implementation of the solution. This is the establishment of a volunteer organization modeled on Estonian CDU[101]. In addition, it is important to develop

[98] *Ibid.*

[99] Czosseck, Ch., Ottis, R., Taliharm, A. Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security. - International Journal of Cyber Warfare and Terrorism, p 24-34

[100] *Ibid., 24*

[101] Wang, K.Ch. The cyber threat landscape: Challenges and future research directions Computers & Security. Toronto: Elsevier Limited, 2011, p 719-731

the cyber units within the reserve military system of Georgia. These two solutions do not compete, they supplement one another.

A volunteer organization should be established under DEA. Thus, this will be a cost-effective solution and is possible to implement immediately. And its practical value will cover issues existing beyond DEA and CERT such as rising of the cyber security awareness, cooperation enhancement between the private and public sectors and knowledge sharing. In addition, volunteer organization will spare DEA from some of its activities and in some cases, can cover CERT. The potential members of the organization will be people from different public and private sectors with a good IT knowledge. If voluntary organization will cover mainly civilian domain the second recommendation concerns the military sphere. Cyber reserve unit is more cost related comparing with a volunteer organization. In addition, Georgian military reserve system is under reform thus, it will be difficult to immediately form cyber units within the reserve system. However, cyber units need to be included in the concept of the future reserve system as soon as it is conceptualized, take on the recruitment and organizational issues. The main goal of the cyber reserve units will be the defense of military information infrastructure and providing specialized services to the armed forces of Georgia. Thus, cyber units will not duplicate the mission areas of the voluntary organization.

To sum up, the recommendations to Georgia will be immediate establishment of a voluntary organization, including cyber units in the concept of the future reserve system and after conceptualization, organizing recruitment and other logistics issues.

SUMMARY

World becomes more and more dependent on information systems and communications. Developing countries become more and more dependent on computer systems. IT advancement brings the security of the vital systems onto focus. Human resources are usually scare in IT field and governments have to spend time and money in order to address the information security and cyber security issues. Thus, the issue of volunteerism comes forward at this time and there are examples of incorporation of volunteers in cyber defense in many countries. Volunteerism usually means self-motivated, uncompensated world. People volunteer to gain skills and experience. There can be various incentives set to attract volunteers. Volunteerism, non-profit activism was one of the major drives for the development of global cyberspace. In late 1980s Computer Emergency Response Team – Coordination Center (CERT-CC) was established to respond to emerging security threats un cyberspace. It was volunteer, non-profit organization and for not it has been transformed into a coordination point of national CERSs of various countries[102].

Cyber-attacks which took place in Georgia in 2008 showed that the country lacked cyber capabilities and was unable to defend its information infrastructure. The shortage of human resources in IT sector is an issue for Georgia and this mater thesis aimed to overcome the manpower issue and to find cost-effective, immediately implementable solutions to develop cyber capabilities of Georgia.

The existing deficit of human and financial resources brings to volunteerism. The volunteerism has been one of the driving forces for the development of Internets, since the first days. Volunteers are actively involved in cyber defense of Estonia. Cyber Defense Unit of Estonia aims to bring Estonian volunteer cyber security expertise together both from public and private sectors. Expertise scope of members spans from programming to information security management and law. Thus, private and public sector and the enormous amount of skilled and experienced experts can have a positive influence on the internet world and can make a

[102] Brenner, S. Cybercrime: Criminal Threats from Cyberspace. Santa Barbara: Praeger, 2010, p 31

meaningful contribution to national cyber security. Volunteers can carry out the essential role in increasing national cyber security capabilities.[103]

Thus, the master thesis explored the example of Estonia and analyzed it for applicability to Georgia. First solution was the establishment of a voluntary organization modeled on Estonian CDU[104]. The legal status of the volunteer organization can be defined as a legal entity of Georgian public law, which excludes any entity to be commercial or profit oriented. The second solution was developing cyber units within reserve military system of Georgia. Bothe of these solutions are affordable for the country and is possible to implement immediately. The solutions provided will not compete for human resources and will not duplicate the mission areas of each other.

Criminalisation of the unlawful activities undertaken in the cyberspace on the level of legislation is a big achievement itself. However, the priority should be given to the fight against this type of crime, charging with the responsibilities and not having so-called "dead" articles in the laws. In order to avoid the issues with the law-enforcement authorities, it is essential to define what exactly needs to be protected – general informational relations or the right of ownership of computer information. This issue is the topic of scientific debate as well. Determination of the reasons for the origination and development of computer crime requires the analysis of current situation, influencing the social-economic and legal development of the society in Georgia.

It is expected that computer crimes will increase in the nearest future. Thus, it is essential to introduce changes to the legislation, as well as adopt preventive measures assuring elimination and avoidance of cybercrime[105].

Volunteerism offers an opportunity to get over the manpower deficit and to find cost-effective ways in order to develop a defensive cyber capability. Volunteer option is very important for small countries like Georgia. Volunteerism for cyber security can be further researched.

[103] Ch. Czosseck, R. Ottis, A. Taliharm, Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security, International Journal of Cyber Welfare and Terrorism, p 24-34

[104] Jayakumar, Sh. State, Society and National Security: Challenges and Opportunities in the 21st Century. Singapore: World Scientific Publishing, 2016, p 17

[105] Chawki, M. Critical Look at the Regulation of Cybercrime, A Comparative Analysis with Suggestions for Legal Policy. Lyon: University of Lyon, France, 2005, p 2-56

Volunteer examples and analysis of the volunteer solutions in relation to Estonia was important to understand all the potential gains offered by volunteerism to cyber defense. The questions with respect to the potential legal and political setbacks should be as well considered. As countries pay more attention to cyberspace, there will be more empirical data available for analysis.

LIST OF REFERENCES

Books

Brenner, S. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Santa Barbara: Praeger.

Carr, J. (2011). *Inside Cyber Warfare*. 2nd ed. Town of Newton: O'Reilly Media.

Friis, k., Ringsmose, J. (2016). *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives.* Abingdon: Routledge.

State, Society and National Security: Challenges and Opportunities in the 21st Century. (2016). / Ed. Jayakumar, Sh. Singapore: World Scientific Publishing.

Cyber Security: Analytics, Technology and Automation. (2015). / Eds. Lehto, M., Neittaanmäki, P. Springe: Springe Punishing.

Kostyuk, N. (2014). *International and Domestic Challenges to Comprehensive National Cybersecurity- A Case Study of the Czech Republic.* San Jose: Henley-Putnam University Press

Tsatsanashvili, M. (2004). *"Information Law".* Tbilisi: Tbilisi Publishing Limited.

Wernberg-Tougaard, C. (2007). *IT-Security Beyond Borders — an Assessment of Trust Levels Across Europe*. Pennsylvania: Unisys EMEA.

Wiener, N. (1989). *The Human Use of Human Beings*. Great Britain: Free Association Books.

Wild, Ch., Weinstein, S., MacEwan, N., Geach, N. (2011). *Electronic and mobile commerce law: an analysis of trade, finance, media, and cybercrime in the digital age*. Hertfordshire: University of Hertfordshire Press.

Articles

Brenner, Sw., Koops, B.J. (2004). Approaches to Cybercrime Jurisdiction. - *Tilburg University,* Vol. 9, 227-239.

Buzan, B. (1997). Rethinking Security after the Cold War. Cooperation and Conflict. California: SAGE Publications, Vol. 32, 5-28.

Cardash, S., Cilluffo, F., Ottis, R. (2013). Estonia's Cyber Defense League: A Model for the United States. Studies in Conflict & Terrorism, Vol. 36, 777-787

Crandall, M. (2014). Soft Security Threats and Small States: The Case of Estonia. - *Defense studies Journal,* Vol. 14, 30-55.

Czosseck, C., Ottis, R., Talihärm, A.M. (2011). Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security. - *International Journal of Cyber Warfare and Terrorism,* Vol. 1, 24-34.

Denning, E. (2010). *Cyber Conflict as an Emerging Social Phenomenon.* Hershey: IGI Global. No. 3, 170-183.

Eichensehr, k.A. (2015). The Cyber-Law of Nations. - *Georgetown Law Journal,* Vol. 103, 319-380.

Gamreklidze, E. (2014). Cyber security in developing countries, a digital divide issue. – *Journal of international communication,* Vol. 20, 200-217

Gercke, M. (2012). Understanding cybercrime: Phenomena, challenges and legal response. - *The ITU publication,* 1-14.

Gyenes, R. (2014). A Voluntary Cybersecurity Framework Is Unworkable- Government Must Crack the Whip. - *Pittsburgh journal of technology law*, Vol. 14, No. 2, 293- 103.

Kaur, N. (2016). Prevention and Control of Cyber Crimes. - *Journal of Computer Science and Engineering*, Vol. 2, 37.

Klimburg, A. (2011). The new Cyber threat: Mobilizing Cyber Power. - *Journal Survival,* Vol. 53, No. 1, 41-60.

Koops, B.j. (2010). The Internet and its Opportunities for Cybercrime – *Transnational Criminology Manual,* Vol. 1, 744-745.

Kozlowski, A. (2014). Comparative analysis of cyber-attacks on Estonia, Georgia and Kyrgyzstan. - *European Scientific Journal,* Vol. 3, 54-63.

Lorents, P., Ottis, R., Rikk, R. (2009). Cyber Society and Cooperative Cyber Defense. *Berlin: Springer-Verlag Heidelberg,* Vol. 5623/2009, 180-186.

Mahrouqi, A., Abdalla, S., Kechadi, T. (2015). Cyberspace Forensics Readiness and Security Awareness. - *International journal of advanced computer science & applications*, Vol. 6, No. 6, 123-127.

Oconnell, M.E. (2012). Cyber Security without Cyber War. - *Journal of conflict and security law,* Vol. 17, No. 2, 187-209.

Randell, B. (1972). On Alan Turning and the Origins of Digital Computers. *Edinburgh: Edinburgh University Press*, 3-20.

Simpson, B., Murphy, M. (2014). Cyber-privacy or Cyber-surveillance? Legal responses to fear in Cyberspace. *Jurnal Information & Communications Technology Law. London: University of New London*. Vol. 23, No. 3, 189-191

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. - *European Journal of Criminology*, Vol. 2, 407-427.

Wang, K.Ch. (2011). The cyber threat landscape: Challenges and future research directions Computers & Security. *Toronto: Elsevier Limited.* Vol. 30, 719-731.

Zekos, G. (2002). Cyberspace and Globalization, Legal problems in cyberspace. - *Law, Social Justice & Global Development Journal,* Vol. 1.

Electronic source

Appazov, A. (2014) *Legal Aspects of Cybersecurity.* Accessible: http://justitsministeriet.dk/sites/default/files/media/Arbejdsomraader/Forskning/Forskningspuljen/Legal_Aspects_of_Cybersecurity.pdf, 18 December 2017.

Basilaia, M. (2012) *Volunteers and Cyber Security: Options for Georgia*. Accessible: http://csbd.gov.ge/doc/Volunteers%20and%20Cyber%20Security%20-%20Options%20for%20Georgia.%20Mikheil%20Basilaia.pdf, 18 December 2017.

Chawki, M. (2005) *Critical Look at the Regulation of Cybercrime, A Comparative Analysis with Suggestions for Legal Policy.* Accessible: http://www.droit-tic.com/pdf/chawki4.pdf, 18 December 2017.

Choucri, N., Madnick, S., Ferwerda, J. (2013) *Institutional Foundations for Cyber Security: Current Responses and New Challenges.* Accessible: http://web.mit.edu/smadnick/www/wp/2010-03.pdf, 15 September 2017.

Dowling, S., McGuire, M. (2013) *Cyber Crime: A review of the Evidence.* Accessible: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf, 12 May 2017.

Fingal Volunteer Centre, Definition & Principles of Volunteering (2017).Volunteerfingal. Accessible: http://www.volunteerfingal.ie/index.php/organisations/articles-for-organisations/165-definition-a-principles-of-volunteering.html, 15 February 2017.

Full-scale aggression of the Russian Federation against Georgia (2009). Government of Georgia. Accessible: http://www.civil.ge/files/files/GeorgianGovernmentReportWar.pdf , 23 March 2017.

Hadzi-Miceva, K. (2006) *Comparative Analysis of European Legal Systems and Practices Regarding Volunteering.* Accessible:

http://www.ecnl.org/dindocuments/203_Analysis%20of%20Volunteer%20laws%20and%20practices_EN.pdf, 18 December 2017.

Haddick R. (2011) *How Russia Pioneered the Use of Cyber-attacks as a Military Tactic.* Accessible: http://www.foreignpolicy.com/2011/01/28/this-week-at-war-lessons-from-cyberwar-i/ 20 January 2017.

Jahankhani, H., Nemrat, A., Far, A. (2014) *Cybercrime classification and Characteristics.* Accessible: http://cdn.ttgtmedia.com/rms/security/Cyber-Crime-and-Cyber-Terrorism-Ch12.pdf, 17 December 2017.

Net Losses: Estimating the Global Cost of Cybercrime (2014). Center for Strategic and International Studies. Accessible: http://www.sbs.ox.ac.uk/cybersecuritycapacity/system/files/McAfee%20and%20CSIS%20-%20Econ%20Cybercrime.pdf, 18 December 2017.

Ottis, R. (2011) *Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability.* Accessible: https://ccdcoe.org/multimedia/theoretical-model-creating-nation-state-level-offensive-cyber-capability.html, 18 December 2017.

Pöysti.T. (2016) *ICT and Legal Principles: Sources and Paradigm of Information Law.* Accessible: http://www.scandinavianlaw.se/pdf/47-26.pdf , 17 May 2017.

Sabanci Cad S., Fuad Paşa Yalısı M., Tersane E. (2014) *Organization of the Black Sea Economic Cooperation, Permanent International Secretariat.* Accessible: http://www.osce.org/cio/128791?download=true, 23 April 2017.

Seven cyber hackers 'stole $45 million in just 10 hours' by draining cash machines in one of world's biggest ever bank heists (2013). Reuters. Accessible: http://www.dailymail.co.uk/news/article-2322062/Seven-cyber-hackers-caught-stealing-45-million-10-hours-second-biggest-bank-robbery-history-New-York.html, 21 November 2017.

Tarkhnishvili, N. (2015) *Two "Keys" is Still Controversial*. Accessible: https://www.scribd.com/doc/142683373/Central-Asia-and-the-Caucasus-2008-Issue-1-49 , 18 December 2017.

The Changing Nature of Cybercrime (2017). International Criminal Police Organization. Accessible: http://www.interpol.int/INTERPOL-expertise/Overview , 23 April 2017.

The Modern History of Computing (2000). Stanford Encyclopedia of Philosophy. Accessible: http://www.plato.stanford.edu/entries/computing-history/#Bab, 23 May 2017.

The Russo-Georgian War 2008: The Role of the cyber-attacks in the conflict (2012). AFCEA. Accessible: http://ww.afcea.org/committees/cyber/documents/TheRusso-GeorgianWar2008.pdf 23 July 2017.

Thoron, L. (2015). *Public Attitudes in Georgia.* Accessible: https://www.ndi.org/sites/default/files/NDI%20Georgia_April%202015%20Poll_Public%20Issues_ENG_VF_0.pdf , 17 December 2017.

Russia 2016 Crime & Safety (2016). United States Department of State Bureau of Diplomatic Security. Accessible: http://ww.osac.gov/pages/ContentReportDetails.aspx?cid=19335, 23 August 2017.

WDS Data Sharing Principles (2015). World Data System. Accessible: http://ww.icsu-wds.org/services/data-sharing-principles, 23 July 2017.

Youth, Volunteering and Employment (2017). International Association of Volunteer Effort. Accessible: http://www.iave.org/about-iave/ , 23 April 2017.

Zubashvili, N. (2017) *CRRC-Georgia: What we know about volunteering in Georgia. Caucasus Research Resource Centers Georgia.* Accessible: http://ww.investor.ge/article_2015_6.php?art=8 , 18 November 2017.

Normative documents

Charter of the United Nations. United Nations. 1 UNTS XVI, 14.10.1945. www.unwebsite.com/charter

Convention on Cybercrime. Council of Europe Treaty Office. No. 185, 23.11.2001. www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

Criminal Code of Georgia. Parliament of Georgia. Legislative Herald of Georgia, Tbilisi, Georgia. No. 2287, 22.07.1999. www.matsne.gov.ge/ka/document/view/16426

Criminal Procedure Code. Parliament of Georgia. Legislative Herald of Georgia, Tbilisi, Georgia. Consolidated version. No. 1772, 29.09.2015. www.matsne.gov.ge/ka/document/view/90034

Georgian Law on Electronic Communications. Parliament of Georgia. 19.05.2011. www.gncc.ge/ge/legal-acts/parliament/laws/saqartvelos-kanoni-eleqtronuli-komunikaciebis-shesaxeb-8082

Georgian Law on Personal Data Protection. Parliament of Georgia. Legislative Herald of Georgia Tbilisi, Georgia. No. 5669, 28.12.2011. www.matsne.gov.ge/en/document/view/1561437

Law of Georgia on Information Security. Parliament of Georgia. Legislative Herald of Georgia, Tbilisi, Georgia. No. 6391, 05.06.2012. www.matsne.gov.ge/en/document/view/1679424

Universal Declaration on Volunteering. International Association for Volunteer Effort. The Netherlands, 15.01.2001. www.fcsh.unl.pt/ensino/voluntariado/DeclaraoUniversaldoVoluntariadodeJaneirode2001.pdf

Annex 1. Statistics by Georgian Foundation for Strategic and International Studies

Registered cybercrime by the MIA territorial and structural units under articles 284, 285, 286 of the Criminal Code

Time Period	Articles 284-286		Article 284		Article 285		Article 286	
	Total	Closed	Total	Closed	Total	Closed	Total	Closed
Year of 2014	163	69	144	62	12	7	7	0
Year of 2015 (First six months)	79	22	70	22	3	0	6	0

Registered cybercrime by the MIA Central Criminal Police Department under articles 284, 285,286 of the Criminal Code

Time Period	Articles 284-286		Article 284		Article 285		Article 286	
	Total	Closed	Total	Closed	Total	Closed	Total	Closed
Year of 2014	43	5	33	3	5	2	5	0
Year of 2015 (First six months)	25	0	17	0	2	0	6	0