TALLINN UNIVERSITY OF TECHNOLOGY
Faculty of Information Technology

IDK70LT

Tamar Tabagari
IVGM146097

GEORGIAN CYBER DEFENSE UNIT

Cyber Reserve

Master's Thesis

Supervisor: Alexander Norta
Associated Professor
Faculty of Information Technology:
Department of Informatics:
Chair of Software Engineering

Tallinn 2016

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Tamar Tabagari

11 May, 2016

Abstract

The thesis is dedicated to develop defensive cyber capabilities of Georgia. It explores the possible options which may bring most effective and fruitful results not only for Georgia and it national security agenda but also for other small and developing countries which have similar backgrounds and inherited problems from the past.

As the main aim of this contribution is to provide the deeper understanding of the current phenomena in ICT field, the methodology used in the thesis is a case-study method based on field and observational studies. It is empirical enquiry that draws on data triangulation of evidence to investigate number of instances of contemporary phenomenon in Cyber Security field in its real-life context. Based on the interviews with field experts we focused on international experiences as the iterative cases and collected appropriate data to process and get the solutions which would ensure sufficient amount of selections for useful and effective proposals.

This paper shows that though cyber security is contingent on a variety of factors that varies by country, Georgia can get best position itself for future improvement by focusing policy on areas that improve technological, social, and economic outcomes to benefit the state.

This thesis is written in English and is 82 pages long, including 5 chapters, 4 figures and 3 tables.

Annotatsioon

Gruusia küberkaitse üksus

Käesolev lõputöö on pühendatud Gruusia kaitsva kübervõimekuse arendamisele. Samuti uuritakse töös võimalusi, mis võiks kaasa tuua kõige efektiivsemaid ja viljakamaid tulemusi, mitte ainult Gruusiale ja Gruusia riiklikule tegevuskavale vaid ka teistele sarnase tausta ja minevikuprobleemidega väikestele riikidele ja arengumaadele.

Töö peamiseks eesmärgiks on anda sügavam ülevaade praeguse IKT sektori fenomenist. Antud töös on kasutatud juhtumiuuringu meetodit, mis põhineb valdkonna uuringutel ja vaatlustel. Tegemist on empiirilise uurimusega, mis toetub arvukate tõendite uurimisel meetodite kombineerimisele, et uurida kaasaegse küberturvalisuse valdkonda reaalse elu kontekstis. Tuginedes intervjuudele valdkonna ekspertidega, keskenduti rahvusvahelistele kogemustele kui iteratiivsetele juhtudele ja koguti asjakohaseid andmeid, mida töödelda ja saada lahendusi, mis tagaks piisava koguse valikuid kasulikeks ja tõhusateks ettepanekuteks.

See töö näitab, et kuigi küberjulgeolek sõltub mitmetest teguritest, mis on riigiti erinevad, siis Gruusia võib saada endale tulevikus parema positsiooni, keskendudes arengutes riigile kasu toovatele poliitikavaldkondadele, mis parandavad tehnoloogilisi, sotsiaalseid ja majanduslikke tulemusi.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 82 leheküljel, 5 peatükki, 4 joonist ja 3 tabelit.

List of abbreviations and terms

ICT	Information and Communication Technology
GDP	Tallinn University of Technology
NRI	Network Readiness Index
ISP	Internet Service Provider
ADSL	Asymmetric Digital Subscriber Line
DSL	Digital Subscriber Line
UGT	United Georgia Telecom
USD	US Dollar
LTE	Long-Term Evolution
CDMA	Code Division Multiple Access
CERT	Computer Emergency Response Team
IOS	International Organization of Standardization
ISACA	Information Systems Audit and Control Association
MOD	Ministry of Defence
MOIA	Ministry of Internal Affairs
MOE	Ministry of Economy and Sustainable Growth
MOJ	Ministry of Justice
LELP	Legal Entity of Public Law
NATO	North Atlantic Treaty Organization
CCD	Cyber Crime Division
TTP	Tactics Techniques and Procedures
FBI	Federal Bureau of Investigation
NCA	National Security Agency
GEL	Georgian Lari
NGO	Non-governmental Organization
DEA	Data Exchange Agency
GITI	Georgian Information Technology Innovation
EU	European Union

G2C	Government to Citizen
G2B	Government to Business
ID	Identification Document
USAID	United States Agency for International Development
UNDP	United Nations Development Programme
WTIS	World Telecommunication/ICT Indicators Symposium
ITU	International Telecommunication Union
NSDI	National Spatial Data Infrastructure
OTRS	Open-source Ticket Request System
IP	Internet Provider
FIRST	For Inspiration and Recognition of Science and Technology
ENISA	European Union Agency for Network and Information Security
NAPR	National Agency of Public Registry
CISM	Certified Information Security Managers
CISA	Certified Information System Auditors
CRISC	Certified in Risk and Information System Control
IT	Information Technology
TFP	Total Factor Productivity
CSIRT/CC	Computer Security Incident Response Team/Communication Centre
TDR	Territorial Defense Reserve
GFR	Ground Force Reserve
GAF	Ground Armed Forces
NRFC	National Reserve Forces Committee
MPs	Members of Parliament
UN	United Nations
DDoS	Distributed Denial of Service
JTF-GNO	Joint Task Force for Global Network Operations
USAF	US Armed Forces
CIA	Central Intelligence Agency
DOD	Department of Defence
CCDCE	Cooperative Cyber Defense Centre of Excellence
OPEC	Asia-Pacific Economic Cooperation
OECD	Organization for Economic Co-operation and Development

OSCE	Organization for Security and Cooperation in Europe
OAS	Organization of American State
UNODC	UN Office on Drugs and Crime
UNGA	UN General Assembly

Table of contents

1.1 Problem statement 11
1.2 Research Objectives 13
1.3 Content 13
2.1 Earlier Studies 15
2.2 Theory 15
2.2.1 Georgian ICT background and inherited problems from the past 15
3.1 Research Method 40
3.2 Research Questions 41
3.2.1 Main Research Question 41
3.2.2 Research Question 1 41
3.2.3 Research Question 2 41
3.2.4 Research Question 3 42
3.3 Cases and Subjects Selection 42
3.3.1 Russian Cyber Attack on Georgian Cyberspace and its implications 42
3.3.2 Create Competencies in Cyber Security Based on Other Countries' Similar Situations/Problems 46
4.1 The evaluation and minimum requirements, which Georgia should satisfy on the international level based on the UN cyber security index 57
4.2 Proposals, Requirements, Constraints 63
4.2.1 e-Training 69
5.1 Summery of Findings 71
5.2 Future Work 72
Appendix 1 – The list of Critical Information Infrastructure 80
Appendix 2 – The State Cyber Security Management Chart 82

List of figures

Figure 1. Revenues of Internet Providers by Companies in 2014-2015 (in GEL) 17
Figure 2. Number of Internet subscribers by the companies 18
Figure 3. Resource Allocation in Defence Budget 2015 36
Figure 4. Resource Allocation in Defence Budget 2016 36

List of tables

Table 1. Targets for the development of innovation and technologies 32
Table 2. ‘Georgia 2020’ strives to achieve the following forecast results by 2020..... 34
Table 3. SWOT Analysis of creating additional national security unit 63

1 Introduction

1.1 Problem statement

The web has set up itself as a political investment. Anyone in today's world with a computer knows the work INTERNET does. It is a main source of a person's who wants to reach out to a global audience. We live in a very dynamic era where we face many challenges as well as opportunities. The change is taking over faster than one could comprehend and it is not so harmless process as it seems from the first sight. Government and its society are expected to work more and with keeping a pace with the fast changing world. However, it is inevitable that every society needs a change, a development being in the culture, mass or technology as well as in communication and security systems. The new generations of governments aim to drive economic and social prosperity and protect cyberspace-reliant societies against cyber-threats [10] . It's not mere assertion that security issues are inherent to technological advancement and in the number of governments' agendas it becomes more and more urgent to address these issues to prevent undesirable and detrimental consequences.

It is a common knowledge that nowadays more and more countries are ready to be involved in the modernization process so called "e-Governance". Maybe, you will not be surprised if you see Georgia among these countries and not only among but there has already been started in the country a preparation process to establish e-Society/Cyber Society[23] . In this process Russia-Georgia war of 2008 played a crucial role to commence significant movements in cyber security in the country. Russia-Georgia war of 2008 was the clear show-case of one of the first cyber wars in our era, which revealed the expected threats, the weaknesses of the country in cyberspace and the urgent need to make the fundamental changes in the development defensive strategy of the country [56] . This war is highlighted as a turning point in relation to change priorities of the government and elevate cyber security among them. Cybersecurity strategy recognizes that the economy, society and governments now rely on the Internet for many essential functions and that cyber threats have been increasing and evolving at a fast pace [10] .

Today, we are in complex and dynamic Web 2.0 environment and Information Technologies are developing with alarming frequency as well as Cyber Security and Cyber Attack fields [4] . Small and developing countries like Georgia are getting involved in these processes and because of the lack of financial, professional and infrastructural resources they have not been able to create the appropriate environment that would ensure sufficient level of security, confidentiality, integrity and availability of information in state.

During the last years the initiatives of the Georgian government authorities to use ICT tools and applications for supporting good governance, strengthening existing relationships, building new partnerships within civil society, and upgrade technical cyber capabilities have had important impact on reforming numerous governmental agencies. With the assistance of development partners, Georgia has already implemented ICT based tools to enhance functionality of various ministries and state agencies (i.e. the Ministry of Internal Affairs, Ministry of Defense, Ministry of Justice, Ministry of Finance, General Prosecutor's Office, Civil and Public Registry, Notary Chamber and others) [23] .

However, the results achieved so far is only a beginning of a long way to go far. There is no doubt that technical development is a big advancement but without appropriate professional human resources it means wasted time and financial resources. My contribution aims to find the solutions, which will ensure improved cyber capabilities of Georgia and sustainable cyber environment in the country.

In the thesis, I analyse Georgian ICT background considering current situation and discussing about existing problems and barriers, which influences on defensive cyber capabilities in Georgia. According to the analyses I offer the most suitable ways creating new cyber defensive strategy and an operation system based of international experience. There are great opportunities like sharing the practice and knowledge from developed and experienced countries, modify and adopt their policies, and follow to their developing steps. It’s not easy way, because it is not just copy and paste approach and needs to work hard to tailor to the field but the capabilities of these counters may it to realize. From this scope of view, Georgia is a good example to show how small and developing country may cope with the problems and keep up with processes caused with development of modern technologies.

1.2 Research Objectives

The objective of this thesis is twofold. One is to examine the cyber capabilities in Georgia and find applicable solutions how to use these capabilities optimally. While, on the other hand, it will be a guidebook for other small and developing countries to create their own Cyber Security Index. This paper will give the opportunity to create a Cyber Security Index (platform, strategy, competency) and the operation model for small and developing countries to step forward and closer to developed countries in cyber defense systems.

The methodology, which will be used in the thesis is a case-study method. It will be empirical enquiry that will draw on multiple sources of evidence to investigate number of instances of contemporary phenomenon in Cyber Security field in its real-life context. The questions will be answered with comprehensive and critical analyze based on existing literature and interviews conducted with experts in this field [1] .

This paper will show that though cyber security is contingent on a variety of factors that vary by country, Georgia can best position themselves for future improvement by focusing policy on areas that improve technological, social, and economic outcomes to benefit the state. In my opinion, the first beneficiary will be Cyber Security Bureau on behalf of Georgian government and maybe also other stakeholders like governmental institutions, which are involved in these issues.

1.3 Content

Throughout the thesis I discuss background and existing situation in ICT field in Georgia, main causes of current problems and a role of the government in this situation to identify problems of cyber security in Georgia as a contemporary phenomenon. One of the main questions the thesis will answer is how to create competencies in cyber security based on other countries' similar situations/problems and how to utilize past international experience in cyber security and adopt it to the Georgia's case. In this regard, based on field and observational studies conducted in the framework of this thesis, our recommendation is to create Cyber Reserve Unit of Georgia on the national level which will ensure the strengthening and developing of national security and national cyberspace defense. Through this recommendations, one of the main initiatives

is to create e-service platform based on e-learning tools – e-training, which will be time and cost-effective for both sides – government and potential cyber reservists as well. Even though, National Cyber Reserve experiences some challenges, the government of Georgia should adopt it because of its numerous significances which are discussed in detailed through this paper.

In the paper a literature will be primary source that will be used, thus peer reviews, research papers and judgments of different experts as well as interviews with experts in the cyber security and cyber security in Georgia.

We believe that the new approaches will yield the desired results, which will be based on sufficient representative selection of case studies.

2 Related Work

2.1 Earlier Studies

As we already mentioned, every day cyber security becomes one of the top priorities for more and more countries. Since countries try to move on electronic governance system, cyber security plays the crucial role in this process. Nowadays, managing cyber security risks and developing proactive strategies for reducing cyber security vulnerabilities becomes top of the hot and urgent topics for countries [2] . Especially, when it is going out from the frames of administrative processes and concerns to military issues like it happened in 2008 in Georgia, we can't just say that it was just a war, it was Cyber War as well [56] . To set out the scheme to help develop the reliable and sustainable environment, which will ensure positioning of Georgia as defensive side of cyber capabilities, we will rely on observational studies on the example of more experienced countries which already have passed this way successfully. Create competencies in cyber security based on other countries' similar situations/problems give us great opportunity to find solutions faster [3] . But it should be mentioned that there is a scarce literature on cyber security issues, so, the peer reviews, the research papers and the judgments of different experts as well as interviews with experts in the cyber security and cyber security in Georgia will be primary source that will be used in this paper.

2.2 Theory

2.2.1 Georgian ICT background and inherited problems from the past

Capital: Tbilisi
Population: 4,935,880 (July 2014 est.)
Area: total: 69,700 sq km ; land: 69,700 sq km ; water: 0 sq km
GDP: 16.52 USD Billion
GDP per capita: 2254 USD
GDP Growth Rate: 2.9%
NRI: 4.2 (60^{th} place out of 143 countries)
e-Participation Index: 0.59 (max. 1, 49^{th} place out of 143 countries)

e-Governance Development Index: 0.6047 (max. 0.9462, 56th place out of 193 countries) [33]

Computerization as well as internetization processes in Georgia started much more later than in Europe or in USA. Before the beginning of 21st century computers were not common good in the country and accordingly, cybercrime almost didn't exist at all. After breaking up of Soviet Union in 1990, each former constituent republic started to declare independence and leave the union one by one. One year later it started revealing an enormous political, economical and social vacuum, which needed urgent assistance and reaction in all aspects. Countries that had enough financial, human and power resources, their conditions allowed them to keep up with developing steps quickly[94] .

However, because of political and economical problems Georgian ICT had a slow start in the country. For years, computer was luxury product and it was accessible for just few people and just in Capital of Georgian, Tbilisi. Positive regulatory development started after the rose revolution in 2003 [22] . It was both political and economical turning point for Georgia. Since 2003, telecom sector influence started increasing on country's other potential developing sectors dramatically. Telecommunications has become one of the fastest growing sectors in the country and its share in GDP reached 7% which meant a lot according to past results. Encouraging a telecom market in Georgia, there has increased a level of internet usage significantly [21] .

Nowadays, situation changed dramatically, there are more than 2.4 million internet users in the country, but Internet accessibility for all over the country is still remained as a problem because more than 65% of internet users comes to Tbilisi [27] . There are still number of regions of Georgia where Internet is not provided or is accessible for little part of rural population. According to Internet World Stats since 2000 till today internet penetration increase from 0.5% to 48.9%, which means that almost half of the Georgian population uses an internet. Number of population of Georgia is 4 931 226. Most frequent and vociferous Internet users are 18-35 year olds, 81% out of them lives in Tbilisi. Population who lives out of the capital - 39% in rural settlements and 61% in other urban settlements, reported that they use internet every day.

As for ISPs, Sanet was first who showed up on the Georgian market in 1993. Four year later, there was second big player Caucasus Network. Although there were only 20 000 users, with 0.5% penetration in 2000, Georgian ICT market potential seemed promising

for other future ISPs. Until 2002 when ADSL services appeared on the market, there was used dial-up technology. Internet becomes second fastest growing sector after mobile services on telecommunication market. In 2006, state-owned telecom operator with cable infrastructure of the country was assigned to Kazakh investor, which it leased to other ISPs. United Georgia Telecom (owned by Kazakh investor) got the monopoly position and all its advantages, which means high rates and strict rules to use its network. In response, soon Sanet, Georgia Online (dial up technology), Caucasus Network (DSL) and Telenet (fixed Wireless) merged as a Georgia's largest internet provider under the name Caucasus Online. Beginning laying down its own fabric-optic metropolitan network, Caucasus Online lessened dependence on the main fixed-line operator, UGT which charged Caucasus Online for USD 110per kilometre to use its network [41] .

	2014	2015
Silkneti	61,660,790	73,980,574
Kavkasus Onlaini	56,488,771.35	59,018,530.21
Akhali Kselebi	7,975,160.03	9,368,276.71
Delta-neti	4,314,774.83	7,936,851.10
Total	130,439,496.21	150,304,232.02

Figure 1. Revenues of Internet Providers by Companies in 2014-2015 (in GEL)

It should be mention that there is no official and reliable statistical data which shows the whole picture of the internet usage development way of Georgia, especially for early days when ICT entered in Georgian. There are only fragmented surveys that allow to gather isolated evidences. Based on this small-scale researches, internet penetration increased from 0.5% to 28.3% in ten years, which means more than 1 million users [27]

Nowadays, there are about 150 Internet Service Providers officially registered. According to Georgian National Communications Commission, major providers are Silknet, Caucasus Online and Akhali Kselebi with 637 050 total subscribers in 2015 up by 3.7% compared to the previous year which was 613 339. In detailed, 38.5% of them belongs to Silknet, 26% to Caucasus Online, 7% to Akhali Kselebi. Among these, fiber-optic technology share is 57%, DSL 28%, Wi-Fi 11%, LTE 2% and CDMA 1%. All other technology subscriptions amounted about 1% [30] .

	2014	2015
Silkneti	241,442	254,253
Kavkasus Onlaini	169,014	166,374
Akhali Kselebi	41,633	43,650
CGC	25,148	25,545
Total	477,237	489,822

Figure 2. Number of Internet subscribers by the companies

As US National Democratic Institute's 2014-year survey, Public Attitudes in Georgia, showed the first source of information for society still remains television with 87% of share [34] . Second most reliable source of information, which includes updated information about political, social and other current events in the country is Internet. From this scope of view, social media plays an important role in discussing and analyzing political and social events in the country. The number of Facebook users in Georgia in 2015 is 1 220 000. Social Networks serves as an important platform for developing and forming of a society opinion, and it is an auxiliary mean for communication and information exchange in Government to Society relations [35] .

According to World Economic Forum, The Global Information Technology Report 2015, Georgia got 60th place with 4.2 index value among 143 countries in Networked Readiness Index. United States and United Kingdom shares 7th and 8th positions, and Estonia ranked 22th place. Compared to previous years Georgia went up with 5 positions while Estonia went down by 1 position. NRI assess how successfully countries use ICT to get most out of its revolution. It is based on six main principles, which includes regulatory and business environment related to ICT; ICT readiness measured by ICT affordability, skills and infrastructure; Usage of ICT with all its benefits by wide society – government, business and population; ICT impact on other sectors; Cycle of benefits caused by ICT; and policy guidance clarity; it measures level of utilization and production of information communication technologies in a country. As for ICT use and government efficiency Georgia ranked on 26th place and 49th place in e-Participation Index. However, according to same report, impact of ICTs on new services and products remain low level so far [27]

It's clear that after Rose Revolution, Georgia has set up itself as "ease of doing business" place by demonstrating clear commitment to reform its political, economic and regulatory environment. Transparency and efficiency became one of the high priorities ensuring improvement of the business climate in the country [15] .

On the way of development from legislative point of view, Georgia has been significantly below the European standards for years. Evidently, in Georgia legal framework, regulating total cyber security and e-government issues, has not existed. There have been some fragmented laws/sub-laws adopted governing certain parts of e-initiatives, different norms on e-government are scattered in separate legislative acts, which in many cases have not corresponded to one another conceptually. Most of the existed laws have been old and been applicable only to paper-based relations thus not covering electronic communications. Nonetheless, last years' progresses in Internet and Information innovation sector seemed very promising for forming and developing e-government and e-society in Georgia [21] .

On the other hand, beside the technological and technical advancements, there is not real advancement without interoperable and up-to-date legislation and regulatory framework. Legislative issues are also at the forefront of 21st century security challenges. Since Rose Revolution in 2003, Georgian government has already

commenced creating, upgrading or making amendments in Laws. Most significant ones are e-Document and e-Signature Law (2007); Law of unified Information Registry (2011); Law of Personal Data Protection (2012); Law of Information Security (2012) [23] .

As for the law of personal data protection, it is set to obtain protection of human rights and freedoms, as well as the right of privacy, in the course of personal data processing. During last few years there are a lot of amendments of the law which highlights the fact of increasing its actualization in the country [22] . These amendments give to the Personal Data Inspector power to control and supervise the data processing by law enforcement agencies. It is related to covert surveillance activities represented by Article 143.1 (a) of the Criminal Procedure Code which includes telephone call eavesdropping and recording. These amendments triggered not only the Criminal Procedure Code, but the Law of Operational Investigative Activities and the Law of Electronic Communications as well which caused discussions among civilians. For covert data processing there is needed two-stage electronic system which requires consent of Data Protection Inspector and law enforcement [22] . To say in other words two-stage electronic system means that Data Protection Inspector and law enforcement have a key for direct access to the data of communication companies. One the one hand, supporters of these changes mention that without Data Protection Inspector, law enforcement officials can't access to the data even after court authorization. While opponents discussing that instead of law enforcement officials this mandate should own to communication companies, on which the government responds that it will be very hard to control these companies, especially when mobile operator are not only national ones and it may be misused for political reasons [24] .

There were made some important amendments in Law of Electronic Communications too, which regards to development and regulation of the competitive environment in the telecommunication sector. The law defines the rights and obligation of the persons and legal entities which use or ensure providing services through the means of electronic communication networks and facilities. It also identifies the function of the Georgian National Communication Commission which is independent regulatory body. One of the implicated changes in the law is that law enforcement entities can copy identifiable data from the channels and store it for two years without an approval of the court and prosecutor's decision. To keep the data there is only necessary to authorize [26] .

Law of Information Security establishes the principals for developing of appropriate and reliable environment for maintenance of Information security, identifies state control mechanism which ensure proper implementation of information security policy and defines the responsibilities and rights for public-private sectors in information security maintenance field. The law is applicable to all legal persons and state institutions which are critical information subjects and all other organizations and agencies which are subordinated or related to them [36] .

The Scope of the Law includes a list of critical information system subjects and the criticality classification which are approved by an order of the Georgian Government based on the draft prepared by Ministry of Justice, Ministry of Defence and Internal Affairs and the State Security Service. Before above mentioned amendment, the list approved by a decree of President of Georgia, based on the project prepared by National Security Council. Except this, there are many amendments carried out in 2013-2015 years [37] [38] [42] .

Other statutes providing by law are rules of information security which call for critical information subjects to adopt internal rule for sufficient commitment of this law, to take inventory to keep all necessary information assets; Duties of information security manager; responsibilities of Computer Emergency Response Team (CERT); Priority cyber threats which may hinder to proper functioning of information security systems. Additionally, the law defines status and functions of Cyber Security Bureau of Ministry of Defence of Georgia. According to the law, all critical information infrastructure subjects should fulfill their settlements following to the standards and requirements established by the International Organization of Standardization (ISO) and the Information Systems Audit and Control Association (ISACA) [22] .

Government approved the the list of Critical Information Infrastructure subjects with a Governmental Order #312 in 2014, which at first, included 39 governmental organizations [5] . Later, to this list was added five more Critical Infrastructure subjects from defense field, which are:

- Ministry of Defence
- National Defence Academy of MOD, LEPL
- Cadets Military Lyceum of MOD, LEPL

- Cyber Security Bureau of MOD, LEPL
- Military Hospital of MOD, LEPL

The list of Critical Information Infrastructure _ Appendix N1

Amendments of the laws aim to strengthen the implementation of the regulation related to internal and confidential use of information in above mentioned entities and generally, to induce conformation processes to the European Convention and activities undertaken towards integration of Georgia with European Union and NATO. However, despite these amendments there remains much to be done [22] .

Number of state agencies and state-owned organizations have launched on the way of building modern information society in Georgia. There are number of successfully implemented initiatives in the field of e-governance. Regarding to the governance of ICT sector in Georgia, there are number of governmental institutions responsible for policy development and implementation [21] .

The State Cyber Security Management Chart _ Appendix N2

2.2.1.1 State Security and Crisis Management Counsel of Prime Minister Office

State Security and Crisis Management Counsel was created under the Office of Prime Minister by the Order N38 of Georgian Government in 2014. Its mandate is to regulate all issues related to the state security to internal and foreign affairs policies, to ensuring stability and a law and order of the state [45] . State Security and Crisis Management Counsel, with power of Premier Minister, obtain an assessment of internal and external threats related to security issues. It discusses on internal and external important political issues which include provision of the state security. It obtains organizing of creating state security and political strategies; It makes decisions on collaboration of Georgia with joint security systems and take part in foreign security events based on acknowledged agreements and signed contracts; It examines drafts of laws and normative acts on state defence and security issues. It obtains monitoring of ministries of Georgia in defence and security issues. It manages crisis situations, which contain potential threats for National interests and obtain its neutralization. After the amendments in constitution, the function of obtaining cyber security of inter-agency coordination of Georgian Government transferred to State Security and Crisis

Management Counsel from National Security Counsel which is subordinated by the President of Georgia. Nowadays, Chair Officer of the Counsel is the Prime Minister, Giorgi Kvirikashvili, which considers that in terms of existing constitution, the request regarding to merging State Security and Crisis Management Counsel and National Security Counsel is inadequate. According to the Law on State Security and Crisis Management Counsel, its permanent members are: The Prime Minister as a chair officer; Minister of Finance; Minister of Internal Affairs; Minister of Defence; Minister of Foreign Affairs and Secretary of Counsel [10] .

2.2.1.2 Ministry of Internal Affairs of Georgia

The Ministry of Internal Affairs of Georgia is one of the main governmental institution which plays an important role in implementation and development of national cyber security policy according to international and modern standards. In 2012 Georgia ratified Cybercrime Conversion of 2001 of European Counsel, which calls for each member country to ensure creation of special unit for combatting against cybercrime and to be 24/7 international contact point like CERT [27] . The document defines the type of crimes committed in cyber space which are considered as criminal offence in all other member states. In the wake of the Convention of European Commission on cybercrime, in 2012 under the MIA's sub-unit Central Criminal Police Department was created Cyber Crime Division, which obtains to identify, investigate and prevent the cases of cybercrime in the country. According to requirements of the convention each member country should have special unit which is responsible for cyber security and prevention of cybercrimes. CCD is recruited with 15 professional staffs and subordinate two sub-divisions: Anti-pornographic and Illegal Content; and the Technological Research and Integration. In addition, within system of MIA Main Division of Forensics-Criminalistics there was created special sub-unit Computer-Digital Forensics which accomplishes the steps for first handling and further forensics of digital evidences [26]

As CCD representative mentioned it becomes harder and harder to fight against the cybercrimes because cyber criminals become more sophisticated. So that "To fight them effectively requires improving technical abilities. To obtain a high qualification in this field requires high level of technical trainings". From this point of view, Cyber Crime Division is ready to involve in trainings and assistance of the sessions of best western

practices in Tactics Techniques and Procedures (TTP) of legal forensic investigation and analysis, rules of effective evidence case preparation, consisting international request for information, assistance and extradition [57] .

Moreover, in 2013 MIA elaborated Strategy on Combatting Organized Crime, which also includes measures to combat against to cybercrime. Another important document drafted by MIA is Standard Operating Procedures on Handling Digital Evidences. This document identifies all special software programs and technical rules which is necessary to search and seize cyber evidences. Capacity building of the its units which are responsible for cyber security is evaluated among MIA's priorities [25] . In considering this statute, it carried out training modules for cybercrime police investigators and national first responders. Training modules include the following issues:

- Legal aspects of cyber crime
- Types of cyber attacks
- Forms of searching and seizing of cybercrime
- Case studies

It should be mentioned that in the process of developing and increasing level of cyber security, the number of international organizations and foreign governments entities are involved in that are ready to give a hand of friendship and partnership to Georgia. MIA cooperates with US Federal Bureau of Investigation (FBI), either European law enforcement agencies and obtain to create competencies of cybercrime fighting measures based on these experienced countries [23] .

In 2014 MIA signed the memorandum of understanding on cooperation with National Security Agency (NSA) of United Kingdom, which includes the issues on combatting against organized crime as well as cybercrime. Additionally, it participated in the project of European Counsel for the Eastern Partnership Countries, called 'Cooperation Against Cyber Crime'. The project went on for three years from 2011 to 2014 and its main goal was to strengthen the capacity of the authorities of Georgian criminal justice to handle more effectively with cyber crimes [44] .

Thus, in 2012, there was implemented bilateral project between Georgia and Estonia, which promotes strengthening of capacity of MIA's operative unites in seizing digital evidences and fighting against cybercrimes [44] .

Among the public awareness rising campaign of MIA, short videos called Identification, which was funded by the US Embassy in Georgia, one of the first series was dedicated to cybercrime. Moreover, different unites of MIA are involved and participate regularly in different international training courses, which helps to increase their qualification in combatting cybercrime. Thus, MIA Police Academy cares and organizes active training sessions on cyber crime and security issues. For example, one of them was held by the aegis of the US Embassy and FBI in 2013 [44] .

2.2.1.3 State Security Service

In July, 2015 there was carried out significant changes in Legislation of Georgia regard to divide security and intelligence agencies from the Ministry of Interior and merged under the State Security Service Agency of Georgia [100] . The main functions of the agency represent

- Territorial integrity and military potential of the country from illegal actions by foreign special part
- Ensuring economic security of the country
- Sovereignty
- Constitutional order protection
- Fighting against corruption
- Fighting against transnational and international crime
- Fighting against terrorism
- Protecting secrets of the state

State Security Service Agency unites number of entities under its subordination. They are Counter-Terrorism Center, Counter-Intelligence Department, Security and Anti-Corruption Department, Operative Technical Department empowered with forensic investigative functions and also have the mandate to carry out detentions. State Security Service has the mandate to define state security regime which includes set of rules, norms and procedures to obtain security and data at high-risk state and private organizations. The list is defined and approved by the decree of the government. Despite the supporters of the amendments, there are some civil society organizations and opposition parties which have critical view and argue that it will not address the problem. The amendments on establishing State Security Service with its all mandates

required funding 36.7 million GEL allocated from the budget of the Ministry of Interior [107] .

2.2.1.4 Ministry of Justice of Georgia

Ministry of Justice is an executive branch of the Georgian Government, which is responsible for implementation development and improvement of e-governance of Georgia. Ministry of Justice, on the one hand, provides legislative activities, and on the other, ensures harmonization of legislation with international legal standards. In this regard, Ministry of Justice is working closely with the Parliament, the Office of the Georgian Government (the Chancellery), relevant ministries, other state and local agencies, as well as foreign and international organizations [109] .

Ministry of Justice ensures provision of efficient and accessible service delivery to the customers. The Ministry has developed a concept of the Public Service Hall and the Community Center, which provides functions of several agencies in one space in order to facilitate efficient service and information accessibility for the customers [109] .

Services at public service halls and community centers are provided by the number of LEPLs and agencies of the Ministry but among them there are two main entities which are responsible for provision and proper working of e-governance of Georgia.

LEPL Smart Logic of Ministry of Justice supports introduction of advanced information and communication technologies (ICT) within the State activities and proper functioning of the Government by means of communication and information technologies [111] .

As for LEPL Data Exchange Agency, it was launched in 2010 under the Ministry of Justice. Its main objective is development of E-governance. The Agency is committed to establish an infrastructure for data exchange and provide implementation of information security policy. Thus, its functions are to promote increasing awareness in society, set ICT standards in public sector pertinent to international standards and work on development of information security policies [112] .

In this regards, DEA launched national Cyber Security Forum. It invites all volunteers twice a year from public and private sector to discuss on existing problems and exchange ideas on modern information and cybersecurity technologies. Except this,

DEA has also developed an extensive contact network and established diplomatic relations on international level. It is approved by the fact that GITI, one of the most influential ICT and IT innovations 8th conference was held in Tbilisi, Georgia in 2015. Purpose of the conference is to explain of information technology significance in terms of creating an engine of growth of socio-economic development in the region. The motto of this year was "Partnerships for Competitiveness, Innovation and Cyber Security". Additionally, in summer, 2015 held workshop on infrastructure protection and responses on cyber incidents that are beneficial not only for the country but also for its neighbors in the Black Sea and South Caucasus Region. The initiative aimed to improve regional cooperation by creating of platform for information sharing, developing common cyber defense tools and increasing trust [110] .

As we already mentioned, the aim of the agency is to support the process of electronic data exchange through coordination, acting as a Georgian governmental gateway, as well as focusing on information and cyber security policies. In order to get closer to EU standards of e-governance, Georgia needs to enhance the institutional and capacity building, to ensure the coordination of e-government development as well as the creation of a legal, regulatory and technical environment. EU experts assist the DEA in this pattern. In this concerns, DEA prepared e-Georgia Strategy and Action Plan 2014-2018 within the Twinning Project supported and funded by EU. The Twinning Project aims to strengthen DEA's capacities that support the implementation of the best and the most suitable e-reforms in Georgia. It addresses the development of an interoperability framework of the country. Under the twining program in November, 2015 there has started second part of the project. Its duration is 18 months and budget is 1.3 million euros funded by EU [23] .

"The aim of the e-Governance is to increase public administration efficiency and quality. e-Governance ensure an easy communication of G2C (Government to Citizen) and G2B (Government to Business), decrease the costs and significantly improve the time-efficiency of internal operations. Moreover, increased transparency and quality of public services gets benefit for common wealth. So, e-Governance is considered as a symbol of modern government" – Ivar Tallo, the Resident Twinning Adviser of Georgia in EU Projects [112] .

Project Components are

- Legal/Regulatory Framework

The component is aimed at development of the legal, regulatory framework on E-government (including E-commerce law, information security/cyber security law)

- Interoperability Framework

The component is aimed at establishment of the interoperability framework within which government institutions will use common standards for information storage and sharing

- Knowledge Acquiring

It means acquirement of knowledge and skills in: E-governance, Georgian Government Network Management, and Information Security

- Strategic Paper "E-Georgia"

Development of the strategic paper of E-Georgia and an action plan (roadmap) on E-governance

- Communication Strategy

Adoption and implementation of a communication plan with special emphasis on information security

e-Georgia Strategy and Action Plan 2014-2018 outlines a strategy with concrete action plans and measurable goals leading the public sector to develop a sophisticated ICT nation. The document contains a vision and mission statement in order to present a clear picture of what e-Georgia can achieve through the agreement of a set of strategic priorities for which investments and engagement are ensured [23] .

Vision

The vision of e-Georgia is to become a more efficient public sector offering integrated, secure, and high quality e-Services. Improved usage and participation enable an ICT driven sustainable economic growth.

The vision was further transferred into six mission statements, which have led to eleven thematic priorities for the e-Georgia strategy. The thematic priorities are grouped into Service areas, Future excellence, and ICT enablers [23] .

Thematic Priorities:

e-Services	Infrastructure
e-Participation and open government	e-Security
e-Health	Skills and e-Inclusion
Public Finance Management System	Enabling frameworks and governance
e-Business	Awareness
ICT-Hub Georgia	

The e-Georgia strategy accelerates the speed to become a modern ICT driven nation. Derived from visions and mission eleven priority topics were described and for each topic and subtopic concrete projects and action items with timelines and KPIs are proposed, therefor detailed and measurable goals are defined.

Based on this strategy and action plan for e-Georgia the fundamentals are laid out to develop a more efficient public sector offering integrated, secure and high quality e-Services and enable an ICT driven sustainable economic growth [23] .

To discuss in detail about e-Georgia Strategy and Action plan 2014-2018, we can consider it as e-governance policy of Georgia. It provides a comprehensive and detailed framework for the societal changes enabled by ICT and focuses on the potential fields where the public sector is able to develop and get maxim benefit out of exploiting the full potential of modern information and communication technologies. The general goal of this document is to ensure the prosperous environment for business and civil society based on fields of innovation, which by itself obtains the ICT driven sustainable economic growth of the country [21] .

Creating this kind of document, which defines the concrete acts of government, as well short-term and long-term goals based on ICT means that public sector leads proactively

the development of ICT and found the basis for wealthy and sophisticated ICT nation. It gives the clear picture of the path of development of Georgia addressing to public and private sector.

Additionally, public Service Development Agency and National Agency of Public Registry implemented the project related to the requirements and compliance standards of information security. The goal of project was to implement information security management system within the organizations [23] .

There are presented only part of activities done in recent period by Georgian government. Although we face number of problems and technical issues like lack of infrastructure, lack of internet accessibility in number of regions of Georgia, it is clear that Georgian Government is ready and tries hard to develop, to create advanced governmental system using ICT to address the needs of citizens. As it is shown detailed in e-Georgia Strategy document they are going to increase their involvement in increasing awareness and part of e-democracy, strengthen their effort to create citizen-oriented services and all necessary infrastructures and build the sustainable and strong government by the help of ICT [23] .

Furthermore, the document highlights the importance and the role of each main content of e-governance. It also suggests set of activities and measures to be performed with indication of respective outputs, timeframes and timelines, and suggested assignments of responsible organizational units.

The responsible unit for implementation of this strategy and action plan is DEA [47] .

Beside to this, DEA also holds unit of national CERT under its structure. CERT.gov.ge is responsible to identify and respond on each cyber incident occurred in Georgian public network and critical information infrastructure. At first when this unit commenced operations there was no other similar team in the country, so it was responsible to investigate all cyber incidents. Main functions of CERT.gov.ge are the quick responses on each cyber incident, analyzing of them and making recommendations. there is no doubt that the unit plays an important role in state cyber security and mitigate the number of cyber incidents in the country. In 2014 there was launched new system of cyber incident management (OTRS), by that mean DEA detected 350 cyber incidents in Critical Information System subjects [47] .

During this few yeas CERT.gov.ge gained many important international partners. Worldwide there are several organizations which obtains global network monitoring to identify infected IP addresses. This year CERT.gov.ge commenced close cooperation on this issues and gained the agreement on data exchange with these international organizations. Among these organizations are: ARBOR NETWORKS, SPAM HOUSE, SHADOWSERVER, TEAM CYMRU and et al. In 2014 it got the right to use officially the trademark "CERT".

CERT.gov.ge is a member of different international organizations:

- International Telecommunication Union 2011
- Trusted Introducer – Trusted Backbone of the Security and Incident Response Team Community in Europe 2012
- FIRST – International Confederation of Trusted Computer Incident Response Team 2013

In near future, Georgian CERT is planning to join in European Government CERTs group – ENISA [115] .

In September, 2015 DEA certified to ISO 9001 for quality management system. Its current important implementing projects are:

Trade Facility Systems –the system promotes electronic data exchange among the parties that are involved in transportation and logistics. It saves significant costs and time for preparing requirement documentations which accordingly shortens number of procedures and fasten customer clearance time. The total saving of the project is 4.5 million Gel [49] ;

Mobile Application for Services of Public Registry - NAPR, enables the customers to use the Real Estate Registry services through their mobile phones, plane-tables or other digital devices [48] ;

National Cyber Olympics – CERT.gov.ge of DEA with National Cyber Security has announces start of receiving application for participations. Up to 25 years all young fellows can participate in the Olympics. They should create the groups with at least three members and should register. The Olympics' goal is promotion and popularization

of cyber security sector, revealing and encouraging of young people who are interested in related issues and have appropriate cyber-cognitive skills [48] .

With concern to DEA's personnel and their qualification, its team includes four Certified Information Security Managers (CISM), two Certified Information System Auditors (CISA), one Certified in Risk and Information System Control (CRISC), and one Certified in Governance of Enterprise IT [112] .

2.2.1.5 Ministry of Economy and Sustainable Development of Georgia

One of the main priorities of the Ministry of Economy and Sustainable Development pertinent to the development strategies of Georgia is to create innovative eco-system which directly promotes cooperation with business sectors, accelerate production and creation new jobs, and increasing the competitiveness of Georgia's export. According to Innovative Georgia 2020, which is strategic paper for future development, economic policy of Georgia is based on three main principals. The first one presents obtaining fast and efficient development of the real production sector, which resolves the basic problems of the economy in terms of creating new jobs and reducing the poverty. The second principle implies implementation modern economic policies and improvement of living standards of society. The third one focuses on rational use of natural resources, ensure of environmental safety and sustainability, and prevention of natural disasters during the processes of economic development [50] .

Table 1. Targets for the development of innovation and technologies

Target	Baseline	2017	2020
Knowledge Economy Index ranking	68	55	45
Global Innovation Index	73.0	65	60
TFP (annual %)	2.70	3.00	3.20
Innovation Capacity Index	44	40	36
Global IT Index	65	58	50

It is also mentioned that the cooperation and integration within the European Union is one of the priorities and cornerstone of Georgia's foreign and internal policy.

Correspondingly, for gradual economic integration and political association with EU it is very important to implement effectively Association Agreement between EU and Georgia. To say in other words, execution of all requirement of this agreement is precondition to enable Georgia to position itself among developed countries with economic prosperity [107] .

The main goal of the program of the Ministry of Economy, Innovative Georgia 2020, is to promote utilization of ICT technologies in development of Georgian economy and transfer it as a "green" economy [50] . To achieve the goal, there are number of target points set by the country

- Knowledge Economy Index ranking 45, by 2020, which means to improve position by 23 ranks
- Global Innovation Index 60, by 2020, which means to improve position by 13 ranks
- TFP (annual, %) 3.2, by 2020, which means to improve position by 0.5 degree
- Global IT Index 50, by 2020, which means to improve position by 15 ranks

During this process, the government of Georgia facilitates the development of relevant infrastructure needed for innovation and getting desired results. To building innovation capacity of the country and achieve the targets, in 2014 under the Ministry of Economy and Sustainable Development of Georgia there was established Georgia's Innovation and Technology Agency. It main function is to coordinate and mediate an important role in the country through innovation and technology development. It is one of the first significant steps to transfer country as an ICT regional hub which encourages the penetration of the high-speed Internet Infrastructure and related systems on the national and regional level [23] .

Techno Park is explicit revealing of Innovative Georgia 2020. It is an innovative platform for start-ups companies, which unites industrial parks, innovative laboratories, Fab-Labs, IT incubators. Its mission is to establish innovation and technology eco-system to bring foreign investments and provide Georgian talent with necessary resources [51] .

Tech Park ensures:

- Accessibility of different types of high-tech machines
- Services to develop Start-up companies
- Consultations of experts and high-professionals in necessary fields
- Accessibility of knowledge and experience in terms of innovation and new technologies

The framework of the Innovative Georgia 2020 and the steps already forwarded to achieve the goals settled by Ministry of Economy, look very promising for future development of Georgian 'green' economy and ICT sector as well and should be accompanied by strict metrics to measure the progress [50] .

Table 2. 'Georgia 2020' strives to achieve the following forecast results by 2020

Indicator	Current Rate	Forecast rate
GDP per Capita (GEL, nominal)	5811.7	13 000
GDP per Capita (GEL, in constant price)	5811.7	9200
Gini coefficient	0.41	0.35
Inflation (%)	2.40	3.00
Unemployment (%)	15.00	<12
Taxes (%of GDP)	24	25
Exports (goods and services, % of GDP)	45	65
Current account deficit (%of GDP)	>10	6
Public Debt to GDP ratio (%)	34	<40

To wrap up this section, e-Government development in Georgia is on the right way and the level of development is already quite high (Georgia takes 54th place) [32] . Although, it's still not enough to say that system works properly. It should be mentioned that e-services are accessible for little part of population. One of the main reasons is Internet penetration over the country, there are still number of regions of Georgia where Internet is not provided. The main task of electronic government is that equally all citizens should be able to get the benefit from services. According to qualified and experienced formers' examples when the "electronic government" has been evolving, firstly they cared about accessibility of the computers and Internet. However, in Georgia it is maybe on the contrary, they are starting from creating services. Unfortunately, without accessibility the main goal can't be reached [32] .

Except this, public executive bodies are involved in creating and deployment quite many e-services, they create the digital development strategies and plans but Parliament of Georgia has not officially declared its convention and ratification of idea on electronic government of Georgia yet. There is only on the public discussion level, which means that timelines of execution are not fixed, so authorities under the electronic government cannot have any obligations to provide all services in time and with proper quality. There is no doubt that e-government doesn't mean just infrastructure, platform, web applications, web pages, and service portfolios. It is important for citizens to create such systems, which ensure opportunities of increasing knowledge, awareness, employment, security, socio-economic prosperity, receiving services on time, meeting the social needs, and creating social capital. The strategy, which we have already examined above mostly includes technical issues and there is no presented the real benefits of citizens in case of well-functioning of e-government in Georgia [46] .

On the other hand, Georgia has really great potential to be among top countries that already use the ICT tools and systems to manage the countries in a better way. It should continue working hard and even harder to achieve the goal and build strong and prospered state.

2.2.1.6 Ministry of Defence of Georgia

In the Ministry's Vision, strategic and guiding document of the Ministry of Defence, is provided the development priorities for Armed and Defense Forces. It reflects and promotes the same national values and interests defined in National Security Concept of Georgia. The priorities are consistent with strategic defense reviews of NATO and other partner states. To develop, to ensure transformation to modern forms and to strengthen fully interoperable and professional armed forces of Georgia, which would be capable to participate in EU-led, NATO-led and other international missions and operations, Georgia implemented NATO-Georgia Substantial Package from the NATO 2014 Wales Summit. [45] It promotes to develop a progressive organizational climate of Armed and Defense Forces in the country. According to the report, main directions of the MoD for 2015-2016 are:

- Improved Defense Capabilities

- Streamline Defense Management
- Enhanced NATO Interoperability and International Cooperation

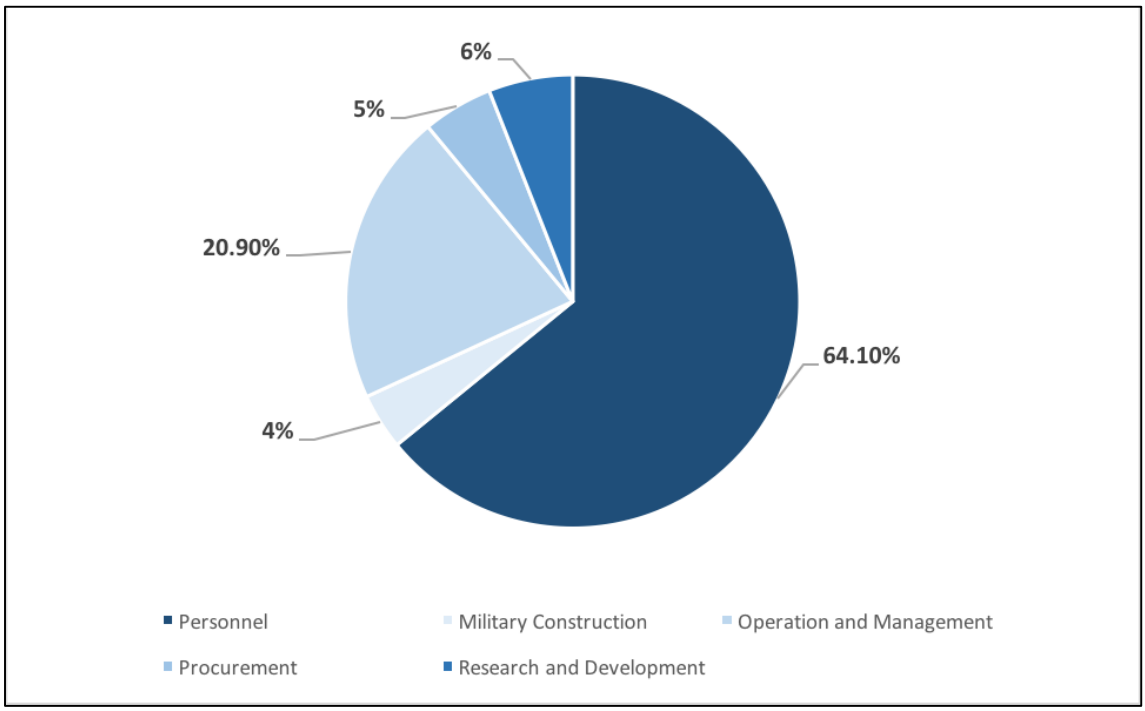


Figure 3. Resource Allocation in Defence Budget 2015

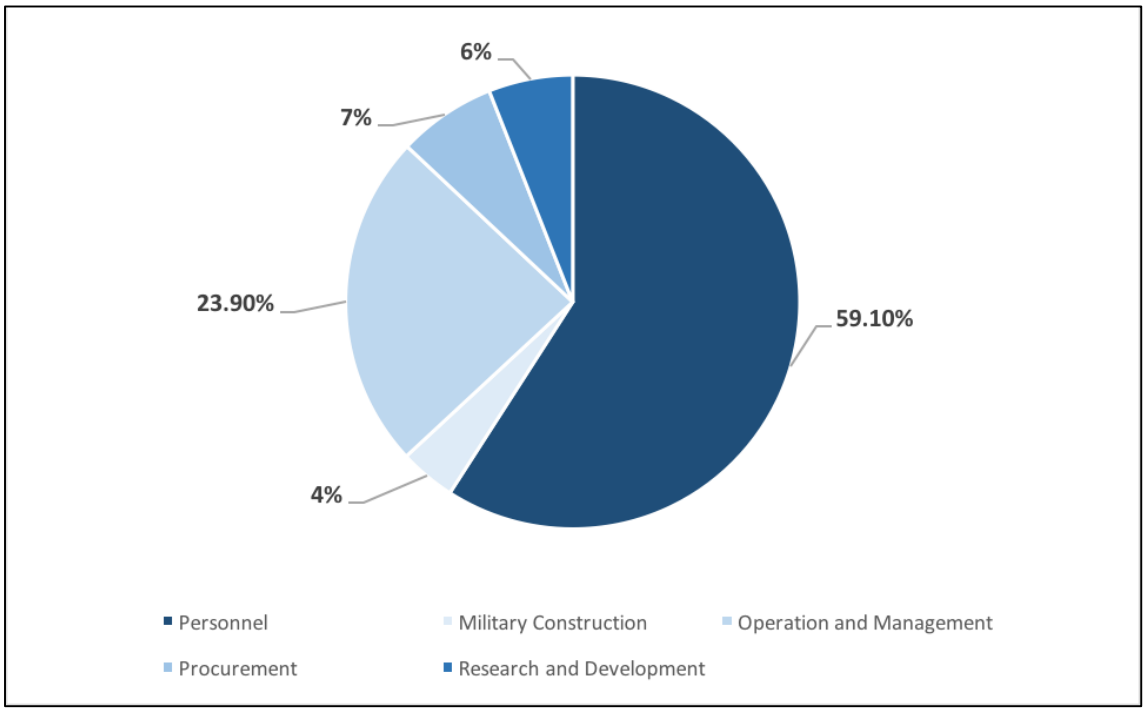


Figure 4. Resource Allocation in Defence Budget 2016

On 24th of December, 2013 Georgian Parliament obtained the amendment of the Law on Information Security about creation of Legal Entity of Public Law 'Cyber Security Bureau' under the subordination of Ministry of Defence. The Bureau is responsible for providing stabile, effective and secure information and communication technology systems for civil office of MoD of Georgia, structural sub-units of Military Forces of General Staff and for all other LELPs which subordinates to Ministry of Defence [22] . The main objective of the Bureau is to obtain development of cybersecurity joint policy, security of information and communication technology system in defense sector, implementation and operationalization of mechanism of computer security incident response in 24/7, which includes three sub units CSIRT, CSIRT/CC and Call Center 24/7, protection from cyber threats and wane cyber risks of all critical information infrastructure under the defence entities of Georgia, initiation and harmonization of Georgian legislation with international legal frameworks, capacity building of awareness in cyber security fields, establishment of densely relationships on national and international levels, and qualification and high professionalism in military personnel pertinent to international standards of cyber security [108] .

Computer Security Incident Response Team (CSIRT/CC) ensure to receive the notifications on cyber incidents in advanced defined means (emails, voice mail, digital sensors, network sensors, electronic questionnaire), to register them in the special system of incident management and to sort them, which includes following steps: verification, primary classification and distribution. The process of verification aims to identify the incident to cyber incidents, primary classification is carried out due to define critical level of the incident. At last, information is provided to responsible team for responding on incident accordingly [108] .

After that Computer Security Incident Response Team (CSIRT) obtain to prevent cyber incident as soon as possible. The cycle of this process contains following steps: data analyzing, choosing methodology for prevention measures, defining necessary resources and action plan, prevention/rehabilitation. After these actions, it is necessary to realizing and archiving all incidents as lessons learnt for future improvements of methodologies [22] .

Georgian Military Reserve System

In 2006 the Parliament of Georgia made significant changes in the Law on Military Reserve Service implement new system of military reserve. However, Russia-Georgia war in 2008 revealed precisely the weaknesses and gaps in reserve system. As security experts assesse the system was unsuccessful and needs more accurate and reasonable changes to make it operable in en efficient way [92] .

It was compulsory for all Georgian males between 27 and 40 ages who were physically able to serve. Males from 18 to 27 ages could serve in reserve voluntarily. Females were premised from this duty. The compulsory period for reserve was 45 days a year. The contracts were signed for 4 years [25] .

In 2012, the Parliament of Georgia discussed new military reserve service concept. According to the draft of new Concept of Defense Reserve System of Georgia, it would be divided in components – Territorial Defense Reserve and Ground Force Defense Reserve. TDR would be based on territorial principle under the command of National Ground Department of Georgia and would be voluntary. As for GFR, it would be under the command of Land Forces of Georgia and would train with them. It would be staffed by former regular army serviceman and would be compulsory. However, voluntary reserve would be possible for others [100] .

Among National Security Concept frames, the elaboration process on formation effective and operable Georgian Reserve System has not finished yet and still continues. New concept of Reserve System is base on the following concepts:

- Simplicity and flexibility in completing and forming of organizational structure
- Accessibility of human, financial and material resources
- Effective mobilizing system
- Proper equipping and training policy
- Compatible command and control systems with current Georgian Armed Forces
- Compatible tasks of reserve with GAF operational requirements

Several weeks ago, the Ministry of Defense announced new concept of Mobilizing and Reserve System, which defines three types of Reserve of Georgia: Ground Force Reserve, Territorial Reserve and Specialists' Reserve. As the author of the draft concept, colonel Shalva Chubinidze stated, it aims to strengthen the defense capabilities

of the country with reserve systems. The document is elaborated under the experience of partner developed countries, including NATO National Reserve Forces Committee (NRFC). The author also highlights the necessary and significant amendments in normative data for implementation and operation of Mobilization and Reserve Systems [102] .

On the third working meeting of discussion on Mobilizing and Reserve Draft Concept, the Minister of Defence of Georgia, Tinatin Khidasheli stated:

> *"We have been discussing the project for month and a half. Currently we are in an interim period. That's why we presented it to the MPs. At the end of May, we plan to present the complete version of the Mobilization and Reserve Concept to the society. I hope we will reach a consensus and the attitudes towards the concept will be similar as this process is needed support and enthusiasm from the society. Reserve is a union of army and society. If this unity isn't created than none of the projects will be successful. Thus, consensus and unity is very important in this process"*

In the process of elaboration of the document, military and security experts with different NGOs were involved. The Ministry of Defense also plans to hold the meeting with different groups of society to introduce the draft concept [99] .

3 Case Study Design

3.1 Research Method

As the main aim of this contribution is to provide the deeper understanding of the phenomena, and it may generate different results on for next studies which are not controlled experiments, the methodology used in the thesis is a case-study method based on field and observational studies. It is empirical enquiry that draws on data triangulation of evidence to investigate number of instances of contemporary phenomenon in Cyber Security field in its real-life context. Based on the interviews with field experts it is revealed that we should have focused on international experiences as the iterative cases and collected appropriate data to process and get the solutions which would ensure sufficient amount of selections for useful and effective proposals. In these regards, according to suggestions from professionals of the field, we chose three main actors and pioneers in cyber defense field – USA: Army Cyber Command; UK: Joint Cyber Unit (Reserve); and Estonia: Estonian Defense League; as source for information. Moreover, the peer reviews and archival analysis was part of data collection with searching literature to identify and strengthen the linkages among studied objects [1] . To assess and ensure the transferability in case study that prevailing environment and conditions of Georgia are similar to another situations of studied objects and the findings are justifiably applicable for Georgian settings we attempted to obtain sufficient details of the fieldwork content and demonstrated the whole and real picture of the phenomena which addressed the credibility of our study [121] .

According to Robson which defines the case study as: “a strategy for doing research that involves an empirical investigation of a particular contemporary phenomenon within its context using multiple sources of evidence”, the main purpose of our study was to find out the situation in Georgian ICT and national defense sector, search for new insights and generate for ideas and hypothesis for new research like e-training approach based on action-design research in cyber reserve system developing. From this point of view, we identify our core research strategy used for as exploratory purposes, but also as for descriptive purposes because it includes the description of the current situation [1] .

As for taking into account the conditions, that may be changed during and/or by the end of the research, we did not set fixed design of the study, rather than we used flexible

case study design which allowed us to change key parameters during the course and adjust the findings of the study. For example, beginning of the research in December, 2016 according to the official side of the Georgian government, it was planning to start pilot project of the Cyber Reserve in May, 2016. As it is known there are some inquests and preparation process has been initiated by the MOD of Georgia but still the details and certain activation plan is not clear [108] .

Because of the fact that this is the qualitative study, the cases discussed in the paper are selected for certain purposes rather than sampled from general population. The replication of the research will ensure to find similar results and create applicable competencies in national cyber defense system for other small and developing countries.

The questions are answered with comprehensive and critical analyze based on existing literature and interviews conducted with experts in this field.

3.2 Research Questions

3.2.1 Main Research Question

How to create a Cyber Security Index (platform, strategy, competency) for small and developing countries?

3.2.2 Research Question 1

How to identify problems of cyber security in Georgia as a contemporary phenomenon?

- What is the background and existing situation?
- What is the role of Georgian government in this situation?
- What are the main causes of current problems in ICT sector of Georgia?

3.2.3 Research Question 2

How to create competencies in cyber security based on other countries' similar situations/problems?

- What is the international experience with cyber attacks?
- What are the minimum requirements, which Georgia should satisfy on the international level based on the UN cyber security index?

3.2.4 Research Question 3

How to utilize past international experience in cyber security and adopt it to the Georgia's case?

- What are the requirements, constraints and proposals?
- What kind of approaches are mostly suitable for Georgia? How should Georgia do it?

3.3 Cases and Subjects Selection

3.3.1 Russian Cyber Attack on Georgian Cyberspace and its implications

There is no doubt that Russian attack on Georgian cyberspace in 2008 was turning point for the country in terms of identifying its significance for Georgia and all other countries. It revealed the weaknesses and problems in defense systems of the country, especially in terms of cyber defense and defense of critical information infrastructure.

Russia did not start its new generation warfare with military operations similarly like it did in 2007 in Estonia [117] . Rather it attempted to achieve its goals through information warfare, intimidation, destabilization and so on. This strategy allowed Russia to form the conditions and strengthen the positions in which they could use military [118] .

According to security experts, the Russian cyber attack in 2008 on Georgia was one of the first case in history of coordinated cyber warfare accompanied with major conventional combat actions. It was regarded as not only Russia-Georgia was 2008, but either contemporary example of Cyber War. Russia invaded Georgia on four fronts, the first three ones were conventional – kinetic warfare and the fourth one was the new form – cyber warfare - the attacks were held through cyberspace [52] .

As an Internet security firm reported the first distributed denial of Service attack (DDoS Attack) against Georgian websites was carried out on 19 July, 2008, several weeks before Georgia-Russian conventional war started. Denial of Service attack is a cyber attack deliberated to prevent the legitimate use of a computing resources. When this goal is achieved by several computers, A Distributed Denial of Service attack has

occurred which means that there was provided more Internet traffic that system can handle which goes the server out of the control and causes its unavailability [56] .

From the first sight, the security and cyber experts didn't have a clear evidence to prove that the government of Russia was involved in cyber assaulting activities directly or indirectly and it was unclear whether the perpetrators were state or non-state actors [57] . However, the fact that the alleged counterattacks occurred only several days prior and it was repeated again one day before the ground attacks has led many security experts to assume that activists knew in advance about the date of the invasion [56] .

An organization of 100 private and public security experts of US, under the Project Grey Goose, investigated the cyber attacks and Jeff Carr, investigator of the case declared: "Level of advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the assault by officials within the Russian government". Grey Goose member neither agreed existing direct links between Russian hackers and Russian Government, nor refuse such possibility of connections [60] .

In the first phase, it was Georgian government and media websites targeted. Russian used botnets which was relied on brute force to carry out DDoS attacks on target units of Georgia. Their cyber attacks on military and governmental institutions websites were very successful. Due to low resilience and fragile nature of Georgian networks it was hard for Georgia to handle Russian cyber threats, especially when there was no any CERT or cyber defense unit in the country [56] .

In next phase, Russian hacker continued to attack on Georgian cyber space but by this time they attempted to broaden their target list. As a result, they there were about 54 Georgia websites down including businesses, financial institutions, educational institutions and even Georgian Hacker websites. The type of attacks consisted with not only DDoS attacks but also defacement activities. For example, it was used US IP address ".com" to command and control (C2) a DDoS attack on the website of the President of Georgia. Instead of the original content of the website there was uploaded a propaganda poster of the President of Georgia, Mikheil Saakashvili [60] .

The Ministry of Foreign Affairs of Georgia blamed Russia for the attacks, while others pointed to Russian Business Network considered as under the influence of Russian Government. In this response, one of the Internet journalist tried to joint Russian

hacktivists following the rules on their website, downloaded prepackaged software, which enabled him to join in the attacks. He assumes: “In less than an hour, I had become an Internet soldier. I didn’t receive any calls from Kremlin operatives… Paranoid that the Kremlin’s hand is everywhere, we risk underestimating the great patriotic rage of many ordinary Russians, who… undoubtedly went online to learn how to make mischief, as I did. Within an hour, they too could become cyber warriors.” [60]

As a result of theses attacks, Georgia found out itself as a cyber-locked and isolated from other side of the world and barely transferred the information. Georgia could not communicate through internet with inter-institutions as well as to the worldwide. Meanwhile, Georgian Government was supported by the US private industry, Estonia and Poland. It made a decision to relocate its critical information infrastructure on foreign servers. According to some security experts, the decision was reasonable and good maneuver which led Georgian Government to way out from the critical situation. While others argued the outsourcing the services in this kind of critical situation would increase the security issue not only for Georgia but also for countries which positioned itself as a Cyber Neutral territory and led cyber refuge to use with its services [60] .

Nonetheless, this means that Russian government had an interest in maintaining or tolerating proxy and empowered organizations that could be implicated in these kind of activities and forms of attacks, such as DDoS, which is not too hard task for an average computer user with right tools [53] .

These conflict revealed the holes not only on national level of Georgian cyber security but also on international level such as an emerging form of conflict, cyber war and cyber neutrality which are not precisely addressed under current international law [60] . There is no clear assertion whether forms cyber attacks like DDoS attacks are legally considered as a “weapon”, or whether cyber attacks are legitimate acts of “armed” conflicts. Accordingly, former head of cyber security for Israeli Government, Gadi Evron states: “This is not warfare, but just unaffiliated attackes by Russian hackers.” Additionally, Bobbie Johnson of The Guardian made a comment that “Many of these strikes seem to be cases of so called ‘hacktivism’.” [60]

However, the Assistant Director of the US Federal Bureau of Investigation’s Cyber Division stated that the FBI is “seeing an increase in the use of botnets… to commit

cybercrime." In this regard, some sceptics point out that there is no clear definition of cyber weapon in legislation on the international level, even the 2001 Counsel of Europe Convention on Cybercrime skips the definition of the terms "cyber attack" and "cyber weapon" [15] . Although cyber conflict issues remain actual, the international law community attempts to unite around the general concept that use the Internet as a mean to carry out the cross-border cyber attacks violates the principals of neutrality. Legal Scholar, Devis Brown comments: "When an information packet containing malicious code travels computer systems under the jurisdiction of a neutral nation, a strict contraction of the law of neutrality would result in that nation's neutrality being violated." [15]

According to Alexander Klimburg, in his study 'Mobilising Cyber Power' he mentions that the Russian security entities often recruit cyber criminals and hacker patriots. Many of them latter operate as "Anti-Russian forces" with the support of security services. As Tomsk FSB Office considers, there is no illegal activities except the expressions of their political positions, which are worthy to respect [53] . Although there are more classified intelligence views, they are beyond the scope of this paper. But one is clear, that every phase of conflict with Russia are based on weakness of internal security system or societal cohesion [118] .

To come back to the Russian-Georgian War 2008, it revealed not only the mistakes Georgia made during the war and problems which existed in neighborhood relations but also the urgent needs of building cyber capabilities to defend the critical information infrastructure and recourses of the country. For developing cyber capabilities, it is not enough to ensure infrastructure, without high professional and skilled manpower it is wasting time and financial recourses. However, there is no doubt that the war 2008 played a crucial role and had a significant impact on the cyber security perception in Georgia. It set itself as a political investment. Since then it became one of the priorities of the government and appeared in strategic documents of national security agenda of the country. [55]

3.3.2 Create Competencies in Cyber Security Based on Other Countries' Similar Situations/Problems

3.3.2.1 USA: Cyber Reserves in USA

Primarily, the cyber reserve in the United States of America is a connection that aims at joint manipulation. This interaction is unified different departmental units. The fundamental significance of this was to curb insecurity as well as to promote good working rapport. In carrying out this, there is a profound creation of a cyber reserve, which is joint and is essential in contributing to security within the nation, appropriate of selection of candidates with the technical and technological knowledge, skills, aptitudes and experience [74] .

The cyber forms that were implemented between 2010 and 2015 included: cyber security which was developed so as to make the cyberspace safer and reliable. This was for the people in the business departments that were severely resilient to attracts and even crimes from the cyber techniques. Again, there was a great change in the employer advisory board homepage. The restructuring based on the number of the individuals expected to be within a given working environment. Lastly, a significant enhancement was realized in the economic service where the student profiles and documentations were stored. The change done was to sub-divide this section so as to minimize the data loss during cyber hacking [73] .

The U.S. Air Force came up with an idea of creating the 'cyber command' in October 2006. An Air Force Cyber Command was later instituted through a provisional status in November 2006. In Oct 2008, it was decided that the command would not be brought into a life time activation. The Secretary of Defense directed the Commander of U.S. Strategic Command to establish USCYBERCOM. In May 2010, General Keith Alexander wrote a report highlighting his views for the United States House Committee on Armed Services subcommittee [75] .

If the U.S. is taking a formal approach to this, then that has to be a good thing. The Chinese are viewed as the source of a great many attacks on western infrastructure and just recently, the U.S. electrical grid. If that is determined to be an organized attack, I would want to go and take down the source of those attacks. The only problem is that

the internet, by its very nature, has no borders and if the U.S. takes on the mantle of the world's police; that might not go down so well [85] .

Initial operational capability was attained on 21 May 2010. General Alexander was promoted a US Generals, and took charge of U.S. Cyber Command in a function held at Fort Meade that was attended by Commander of U.S. Central Command GEN David Petraeus, and Secretary of Defense Robert M. Gates. USCYBERCOM reached full operational capability on 31 October 2010 [75] .

In July 2011, Deputy Defense Security, William Lynn announced in a conference that "Within Cumberer conscription, a full spectrum of capabilities, but the strategy is meant to offer protection against such threats. the strategy is in a form of five pillars", he said: "When you treat cyber as a domain; employ even more strong and advanced defenses; support the Department of Homeland Security in protecting all crucial infrastructure networks; practice collective protection strategy with allies and international counterparts; and reduce the chances of cyber offenders of committing crime through the web." [82]

In 2013, USCYBERCOM organized an exercise in which reserve officers (who are highly experienced in their civilian cyber-security functions) easily defeated active duty cyber professionals. USCYBERCOM plans to set up 133 teams, with no reserve members. In 2015, Eric Rosenbach, the principle cyber advisor to Defense Secretary Ash Carter, said DoD is considering alternatives to ancient military service [74] .

The command assumed responsibility for several existing organizations. The Joint Task Force for Global Network Operations and the Joint Functional Component Command for Network Warfare were absorbed by the command. The Defense Information Systems Agency, where JTF-GNO operated, provides technical assistance for network and information assurance to USCYBERCOM, and is moving its headquarters to Ft. Meade [74] .

Some military leaders claim that existing cultures of the Army, Navy, and Air Force are fundamentally incompatible with that of cyber warfare. Major Robert Costa, USAF came up with a suggestion of the fourth branch of the military. In reaction to concerns about the military's right to respond to cyber threats, General Alexander stated "The U.S. must fire back against cyber attacks swiftly and strongly and should act to counter

or disable a threat even when the identity of the attacker is unknown" prior to his confirmation hearings before the United States Congress. This came in response to incidents such as a 2008 operation to take down a government-run extremist honeypot in Saudi Arbia. "Elite U.S. military computer specialists, over the objections of the CIA, mounted a cyber attack that dismantled the online forum" [78] .

In the USA today, there is a very significant improvement on the how activities are being carried out. These strategies have been put to take into account insecurity problems. The current situation is that cyber reserves have been jointly formulated to adhere to the inconveniences that may arise. This, therefore, ensures security and the protection of the activities within the nation. Again, it helps in defense department where signals have been used to detect terror attacks. Filling and documentation of given documents have been developed to maintain the economic status. The documents contain information that would rather make the nation deteriorate in its performance. Due to this, appropriate cyber serves have been geared towards maintaining the well being of the citizens by proper storage of their documents [73] .

The organizations are typically found within the domain of the cyber reforms include the learning institutions, the defense and security departments as well as the economic and developmental agencies. The primary and substantial aims of the cyber reserve may involve some issues which include protecting the national security and citizens, the interests, and independence of the country and ensure that the armed forces have sufficient training and are well equipped. In stratification, the cyber reserve has the following focal points to take into account while to carry out its mandate. These coordinators are the strategies that are laid down to be incorporated by the institutions mentioned above [75] .

The main points of the government cyber security strategy are

- Intensifying cooperation within the national and international domains, collaboration element. (Agreement part)
- Comprehensiveness adoption approach
- Strengthening cyber defence though the security organization. (case item)
- Conducting cyber operations through the development of the military capabilities and manageability. (offensive as well as defensive element)

- Intelligence position strengthening in cyberspace. (information element)
- Knowledge positioning as well as innovative strengthening. (adaptive as well as creative part)

Cyber reserve technology has some merits on its usage. First, it dwells mostly on the individual reserves as opposed to the public reserves. This helps in proper updating of the departmental levels thus minimizing the chances of their attacks. It ensures total national security. These points out that some information may be gathered, which aids in the security domain. Again, cyber reserves act as an aggressive and intelligence information gathering. It pinpoints out precisely how sufficient piece of information may be obtained and coherently used in analyzing individual data. Proper cyber technology is used so as to develop a good interacting platform for the same.

Furthermore, cyber reserves resolves in quick recovery of the information that can be put to use so as to enhance communication processes. Lastly, these techniques help greatly in determining crimes that might be committed by certain groups of people [73] .

There are concerns that the Pentagon and NSA might do away with civilian efforts to ensuring cyber security. There are also concerns on whether the command will assist in civilian cyber defense efforts According to Deputy Secretary of Defense William J. Lynn, the command "Will control all daily operations in defense and protection of all DOD networks." Responsibility for federal civilian networks is all left to the Department of Homeland Security. If faced with cyber crimes an order from the executive could expand Cyber Command's spectrum of operations to include, such services as helping the Department of Homeland Security in the enforcement of cyber security [82] .

Being a technological development, the efficiency of the cyber reserves cannot be entirely sufficient. This is due to the numerous challenged that are associated with the same. Among the problems that may be accounted for include the quality manpower. This becomes a problem because there are fewer people who have the capacity of understanding technology. According to this, therefore, including cyber reserves becomes a big problem when comes to its implementation. The technique requires funds and capital to becomes a big problem when comes to its implementation. The technique

requires funds and capital to implement and therefore a very significant amount of money should be put in place for its initiation and maintenance. This makes it expensive and therefore not useful in its totality. Finally, cyber reserve makes proper use of the internet access. Failure to this makes the process less efficient because there would be no any other way of communication [74] .

The reason the state decided to create cyber reserve are several. Even though cyber reserve experiences some challenges, the government of USA adopts it because of its numerous significances. Some of the reasons that lead to this adoption include its importance in curbing terror, proper arrangement of data, enhanced tracking of programs, which are business oriented as well as maintaining the economic and educational status of the nation. Additionally, as the U.S Department of Homeland Security announced the idea came from a task force launching Cyber Reserve to address what was a weak spot for long time – recruiting and retraining skilled cyber professionals who considered that they could receive a better jobs and earn higher salaries in the private sector.

The following characteristics depict the desired features of the cyber reserves according to USA [75] :

- The cyber reserves must be work together. Togetherness promotes unity among the different departments that formulate the reserves
- The reserves must have some tasks to carry out and implement. These must be in good agreement the national strategy and development
- The cyber reserves should meet most if not all, the needs of the citizens
- The cyber reserve should work within certain known domains

The cyber reserves play a vital part in the government of USA. Activities stipulated by the government house numerous advantages that come as a result of using this technique. It is, therefore, clear that to maintain good rapport with citizens, the government of USA has this informative domain that helps her upkeep the records. The skill also adopted aids in economic development and therefore maintaining he economy of the nation. From the information highlighted above its clear that the united state of America has taken a huge strike towards improvement of cyber security. Cyber crime is

an international threat an unless we act abruptly we might suffer radical consequences [84] .

3.3.2.2 UK: Joint Cyber Unit (Reserve)

Every day the UK faces threats to its computer systems and these threats are done by anyone ranging from terrorists to individual activists. In numbers, 93% of the large businesses and 76% of small businesses have faced cyber threats in the past year. This is an alarming number and that is why the government has decided to make UK one of the most secure cyber place in the world and for this to happen, cyber security has to be one of the most important parts of the government. The government therefore wants to train students to have great skills which will enable them to deal with cyber threats and provide security to the UK and its people [62] .

A cyber reserve in the United Kingdom was created in 2013 as a tri-service unit, which provides people an opportunity to be a part of Maritime Reserves, the Army Reserve as well as the Royal Auxiliary Air Force [61] . Its task is to handle any security threats which are done with computer crime [62] . This is done by providing medical services, training, intelligence, information systems and cyber-operations, which are established and controlled. Furthermore, the Cyber Reserve UK supplies command and control which needed for defense operations abroad [66] .

As mentioned above, the Cyber Reserve began in 2013, when they started recruiting people from a wide range of the society. In 2014, the first recruitments completed their induction phase and by 2016 there is a desire to have enough skilled people in order to fulfill the capacity. There are strict assessment criteria for anyone wishing to joint and special training providers as well as courses have been established to make sure only high skilled people get a place in the institution [63] .

The Cyber Reserve UK is responsible for preparing collective forces for operations, developing collective capabilities in a way where investments are successful and the capabilities are coordinated. Finally, the combined activity is enhanced with the help of concepts, education and training as well as applying lessons Joint Force [66] .

There are several institutions, which make the Cyber Reserve. At the top is the Permanent Joint Headquarters, followed by a Special Forces. Next is the Joint Force

Development and Defense Academy; the Defense Intelligence, the Information Systems and Services; the Surgeon General; the Assistant Chief of the Defense Staff and lastly, the Permanent Joint Operating Bases [66] .

The Permanent Joint Headquarters is responsible for commanding collective and combined operations in the military. The head is the Chief of Joint Operations and among other responsibilities of the headquarters are [67] :

- Preparing and completing collective and multinational operations, which are led by the UK
- Commanding UK Forces, which are working with multinational operations.
- Giving military advice to the Ministry of Defense

The permanent Joint Headquarters is furthermore divided into eight divisions, namely, staff, operations intelligence, current operations, logistics, crisis planning, communication systems, finance and HR, legal and media operations [67] .

The Special Forces is an institution, which is designed to participate in high risk operations on a short notice. They work in very hard conditions all over the world and make sure the safety and security of the British people are well taken care of. In order to achieve this goal, it is very important that the people employed at the Special Forces as well as their techniques, procedures and equipment are well cared for [68] .

The Defense Academy is an institution were people are educated and where most of the command, personnel, technology is provided in a form of a training. They also perform non-technical research and provide assessment as well keep a close link to the international military institutions as well as UK universities [65] .

The Defense Intelligence is responsible for intelligence products, as well as giving advice on decisions concerning policy and commitment and employment of armed forces. They provide information to research about defense and programs on equipment as well as provide support to operations in the military [69] .

The Defense Medical Services take care of the promotion, protection and restoration of the health of its employees in order to make sure they are medically prepared for a mission either in the UK or abroad. It is comprised out of doctors, dentists, nurses, other health professionals, paramedics and support staff [70] .

Lastly, the Permanent Joint Operating Bases provides a physical defense as well as maintaining the UK's domination abroad and providing contributions to the Government Policy of the UK [71] .

There are advantages and disadvantages of the UK Government's Cyber Security strategy. In terms of disadvantages, most employees of the Joint Cyber Unit are not necessarily skilled for the job. Most people who do have the necessary skills to work for the Cyber Reserve demand high salaries, which the UK government cannot afford and that is why they train regular people, even students, to become part of their institution. This is alarming for some people who believe that those employees are not capable of doing the job properly since they are not skilled enough. Another disadvantage is in terms of the scope of the Cyber Reserve. Firstly, there is primary focus on technical requirements while skills such as legal and security skills are a secondary focus or are not even a focus for the institution. Secondly, the Joint Cyber Unit protects the assets of the Ministry of Defense and this gives the institution a very militaristic tone [64] .

In terms of advantages, there are four main topics to pointed out which come with the UK Government's Cyber Security Strategy. Firstly, the government wants to deal with cybercrime and make sure the UK is one of the safest places in the cyberspace as well as provide an opportunity for business to be done in cyberspace. Secondly, the UK will become stronger against cyber attack and will be able to protect the interests of its people in the cyberspace. Thirdly, the UK will enable an open and stable cyberspace which can be safely used by the British people. Finally, the UK will have cutting edge knowledge and skills in order to provide the above mentioned elements [119] .

3.3.2.3 Estonia: The Cyber Defense League of Estonia

Estonia boasts itself as one of the most technologically advanced nations. Estonians developed the code behind Skype, their medical records are stored online and they can use the internet to vote in general elections. The government provides over 600 online service. On the official website of National Defense League, it is stated that "The Cyber Unit's mission is to protect Estonia's high-tech way of life, including protection of information infrastructure and supporting broader objectives of national defense." [92]

The cyber unit is a specialized body of the National Defense League. The National Defense League is a reserve army of volunteers. Ultimately the Defense League is under

the control of the Ministry of Defense. It follows the internal rules and strategic guidelines set by the ministry. It functions as a legal person and its status, structure and tasks can only be changed by changing the law. This makes it a bit different from traditional army units because in some cases it's possible to change their shape internally. The National Defense League is a separate entity from the Defense Force, even though they are governed by the same ministry. Their internal organization, in terms of rank names and symbolism is different. However, there is a vertical chain of command linking them. The Defense League is divided into structural units whose commands are subordinate to the Commander of the Defense League. "The Defense League is managed by the Commander of the Defense League, who is directly subordinated to the Commander of the Defense Forces." [90] So even though they are legally distinct entities they have a unified command chain leading to the Ministry of Defense and their functions and structural arrangements overlap significantly. For example, in the CDU analysis of the Cyber Unit one of their core functions was to strengthen and ensure the security of the population, while one of the supplementary tasks was cyber security assistance. The only difference between these two tasks is the legal question of domain, rather than a substantial difference in the task itself. In the National Defense League Act it is stated that "The Defense League is a legal successor of the defense league established as a self-defense organization on 11 November, 1918." [90] The first version was established during the war for independence and it grew out of the Citizen's Defense Organization, an organization whose purpose was to curb public disorder accompanying the Russian revolution. The second version was established in 2013. Some of the stated objectives of the Cyber unit are promoting international cooperation, informing the public and promoting active citizenship and promoting public-private cooperation. The public private cooperation can be seen in the structure of the unit itself as it employs government specialists as well as other volunteers. The positive side of such cooperation is that it encourages citizens to inform themselves and get involved in government. This creates a higher level of the trust and transparency and has a positive effect on the democratic structures of society. In the official 2014-2017 Government Cyber Security Strategy it is stated that the growing reliance on information technology "will contribute to the improved availability and usability of services, enhance transparency and citizen participation in governance, and cut public as well as private sector costs." [89]

On the other hand, this growth in reliance makes government structures and public citizens more vulnerable to cyber attacks. This vulnerability was clearly seen in a string of attack in 2007. Immediately after the three weeks long string of attacks on both government websites and sites of crucial private sector parties, such as bank, cyber security came to the forefront of the national concerns. In their paper Estonia After the 2007 Attacks: Legal, Strategic and Organizational Changes in Cyber Security Christian Czocceck, Rain Ottis and Anna-Maria Taliharm outline a brief history starting with the 2007, Action Plan to Fight Cyber Crime and ending with the formation of the Cyber Reserve [87] .

What all the strategies outlined in the paper share are a focus on creating government structures capable of defense against cyber crimes and a focus on informing the public about cyber security. In the 2014-2017 strategy one of the key points is the creation of an information constable, a government official whose main functions are investigating cyber crimes and informing the public [89] . The strategy focuses on three main issues:

- Crucial Services
- Cyber Crime
- National Security

It's stated that international cooperation is necessary to ensure handling of these three issues properly and correctly.

The growth of information technology has made the world more interrelated and codependent. Cyber attacks are becoming international, so defense strategies have to follow too. In 2007 string of attacks happened in the middle of the Estonian-Russian disagreement over the relocation of the soviet graves and equipment. In the paper Estonia After the 2007 Attacks, it's claimed that they were politically motivated. Specifically, they claim that Russia commissioned the attacks, but the actual actors, who executed them were of different nationalities, showing the international character of cyber crime. Most of the international cooperation is done through the NATO Cooperative Cyber Defense Centre of Excellence (CCDCE) [91] .

There are yearly Joint Shields exercises and the CCDCE also cooperates with the National Defense Force in research projects and strategy. It is much more than a military organization. It has agreements with academic institutions and private sector.

Its functions as a recruiting platform and resource allocation service are perhaps more important than purely military functions as these functions in particular create public-private links and international links as well. On the official CCDCE website they explain that "The Centre is guided by an international Steering Committee consisting of the representatives of the Centre's Sponsoring Nations." [91]

The other important function is purely strategic. Estonia was formerly part of the Soviet Inion. Placing a NATO Centre in their capital is meant to demonstrate that they no longer wish to be under Russia's sphere of influence and is part of security guarantee. Furthermore, it allows NATO to show Russia its dominance by placing a military object in their 'back yard' [91] .

The cyber reserve seems almost indispensable to Estonian National Security, considering their technologically advanced structures. The recruitment of volunteers allows for ordinary citizens to get involved in governance, which creates trust and active citizenship. However, the direct chain of command between volunteer reserves and professional forces leading to the Ministry of Defense allows the political party in power to manipulate its citizens by setting the strategic agenda for the Defense League. This is especially problematic because the Defense League Act specifically prohibits any political party's activities within the Defense League [90] .

Citizens of Estonia greatly profit from reliable government on-line service and this reliability is ensured by their cyber defense programs and institutions. On the other hand, their growing reliance on information technology makes them vulnerable to cyber attacks. The problem with cyber crime is that it's unregulated, partly because of its international character and partly because of the quick pace with information technology advances. This point is covered in the defense strategy for 2014-2017. Public-private and international cooperation have so far been sufficient in stopping any potential attacks. The education, scientific research and cooperation with specialized bodies implemented through CCDCE set the base for future protection, as well as better services [89] .

4 Results

4.1 The evaluation and minimum requirements, which Georgia should satisfy on the international level based on the UN cyber security index

There are number of intergovernmental organizations which address the issues and set international regulation related to cybersecurity at the policy level. They are [10] :

- Asia-Pacific Economic Cooperation (OPEC)
- Counsel of Europe
- European Union
- G8
- Internet Governance Forum
- North Atlantic Treaty Organization (NATO)
- Organization for Economic Co-operation and Development (OECD)
- Organization for Security and Cooperation in Europe (OSCE)
- Organization of American States (OAS)
- United Nations (UN)
- International Telecommunication Union (ITU)
- International Telecommunication Union (ITU)

The United Nations has hosted actively number of activities related to cybersecurity and cybercrime in the past few years. In 2003, through the resolution 58/32 General Assembly initiated the Secretary-General to discuss on Information Security threats and in this frame launched Group of Governmental Experts. In 2010, through the UN General Assembly resolution 60/45, the GGE introduced the report which included number of recommendations, like “further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructures.” After that there was a working paper prepared by the UN Office on Drugs and Crime (UNODC) among the frame of 12th UN Congress on Crime Prevention and Criminal Justice. The paper included recommendation “the development of a global convention against cybercrime should be given careful and favorable

consideration". There were several resolutions adopted by UN General Assembly related to cybersecurity such as 57/239 on the "Creation of the global culture of the cybersecurity" based on the OECD 2002 Security Guidelines [10] .

In global society, technological developments of cyberspace bring the critical concern of cyber threats and the need to create cyber security measures in protecting against criminal activities. Rapid growth of Information and Communication Technologies has created new opportunities for criminals to perpetrate crime, exploit new vulnerabilities and attack on countries' Critical Information Infrastructure. On the other hand, free flow of information through the internet may ensure higher education, democratic governance, economic and social development as well [11] .

However, the differences in development of information and communication technology levels from country to country can diminish the effectiveness of international cooperation in fighting against cyber criminal activities and get the detrimental consequences for all states. To establish global agreement or Protocol based on United Nations competence, which aims to address global challenges ensuring promotion of peace and security in cyberspace, there is a need to have common understanding of cyber crime and cyber security among all countries. The protocol also includes globally applicable legal frameworks which are interoperable with the existing national legislative measures [11] .

On the World Summit on the Information Society in Tunis, 2005 the following objectives were defined:

> *"We call upon governments in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing framework, for example UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies" and regional initiative including, but not limited to, the Council of Europe's Convention on Cybercrime." (Paragraph 40) [13]*

> *"We affirm that measure undertaken to ensure Internet stability and security to fight cybercrime and to counter spam, must protect and respect the provisions for privacy and freedom of expression as contained in the relevant parts of the Universal Declaration of Human Rights and The Geneva Declaration of Principles." (Paragraph 42) [12]*

OECD studied Guidelines for the Security Information System and Networks of number of the countries and assume that there some key concepts such as the need for a culture of cybersecurity, risk-based approach and the shared responsibility of all participants. The latter analysis revealed that there are some key concepts, which are missed in Guidelines: real-time and resilience.

Real-time concept is mentioned as an extension of the concept of "timeliness" included in the Response principle of Guideline. Generally, 'real-time' is considered at an operational level, as situational awareness in time by Computer Security Incident Response Teams (CSIRTs). It means that to be identified, analyzed and taken appropriate measures to prevent the threat by CSIRTs. However, from this scope of view, cybersecurity no longer requires only timely response to incidents but also real-time network monitoring. [10]

As for resilience, generally it is used as the capacity of the information systems of networks to continue smooth and normal operating despite the incident or unexpected technical problems. The resilience or in another words "business continuity" means that in an open environment some level of risks is accepted and some preparation measure should be taken in advance for incident to occur. So, security management approach also takes risk assessment and management into account.

During the implementation of cybersecurity policy, governments should be prepared to face key challenge which is common for almost all strategies they should fine golden balance between protection the openness of the internet and cybersecurity. [10]

For all developing countries that want to be a part of Information Society and benefit from information technology services, it is necessary to create the strategies on the development of the Protocol for cybersecurity and cybercrime that may serve as a global model of protocol for other developing countries as well, because cyberthreats are global problems and need a global harmonization involvement of all stakeholders. [11]

2012 report of the Organization for Economic Co-Operation and Development (OECD), Analyzing a new generation of national cybersecurity strategies for the Internet Economy, reveals that cyber security policy making is at the turning point, which means

that in many countries it has become one of the first national priorities. According to these strategies, general assessment of governments are followings [10] :

- ICTs and Internet are the essential for social, economic development and for a vital infrastructure formation;
- Cyber threats are evolving and increasing with alarming frequency;

Due to the fact that cybersecurity has a global nature in terms of cyberthreats and interconnected ICT infrastructure, there is necessary to apply a common international approach of cybersecurity. This will be promoted by implementing of international standards and good practices in all the dimensions of cyber security. International standards should be applicable at regional and national levels and compatible at international level. It is very important to exist common understanding of the significance and the meaning of cybersecurity to all. There should be a global response for safe and interrelated information society, and facilitate common definition. In that sense, deployment of international cooperation and national cyber security strategies plays an important role. To say in other words, based on international standards and well recognized good practices promotes to create local know how, which will answer specific local needs by integrated local cultural values in national standards. These approach will allow to optimize the cooperation between the actors and avoid to duplicate the works or efforts [11] .

There are number of common concepts which are shared for all strategies [10] :

- Enhanced public-private cooperation
- Reinforced governmental coordination at policy and operational level
- Improved international cooperation
- Respect for fundamental values: privacy, freedom of speech and free flow of information

To say in a different way, global approach means political, economical, social and technical dimensions, which are united under the systemic security framework. The systemic approach concerns to all actors of the information society. To promote a safe and reliable cyberspace environment in the context of emerging information society is everyone's responsibility. Each actor has his/her role to play in the ICT security chain and its development process. Only systematic and schedulable cybersecurity approach

will allow to address all kind of security issues and challenges at any level of any actor from public awareness to policy makers [11] .

A systemic security framework is consisted by:

- ***Political dimension***

  In National security issues, as well as in cybersecurity and cybercrime issues government readiness and decisions play an important role. It should understand of the needs for defense on regional, national and international level; it defines all necessary measures to be taken to ensure the satisfying level of the ICT and CII security. It should find all necessary resources to develop strategic improvements in ICT security.

- ***Legal dimension***

  Regulatory framework can help to transform the Internet into safer place to wage activities. Integrated legal framework and laws applicable to cyber world should be compatible at international level and operational at the national level. From this scope of view Cybercrime Conversion of European Counsel can be taken as an international reference model to develop legal frameworks. Before that the understanding of way of the interpretation and implementation existing regulations should be taken into account.

- ***Organizational dimension***

  Any size of organization in the country should have understanding of basic principles of ICT security management. For instance, how to manage security in complex and dynamic environment, how to create appropriate organization structure and procedures based on collaboration with legal, law enforcement and technical experts, how to assess potential vulnerabilities and threats and etc.

- ***Technological dimension***

  From this scope of view, to decrease the number of vulnerabilities of cyberspace, there should be clear understanding of related ICT risks, cyber threats, cyber attacks, technical potential of misuse. There should be defined

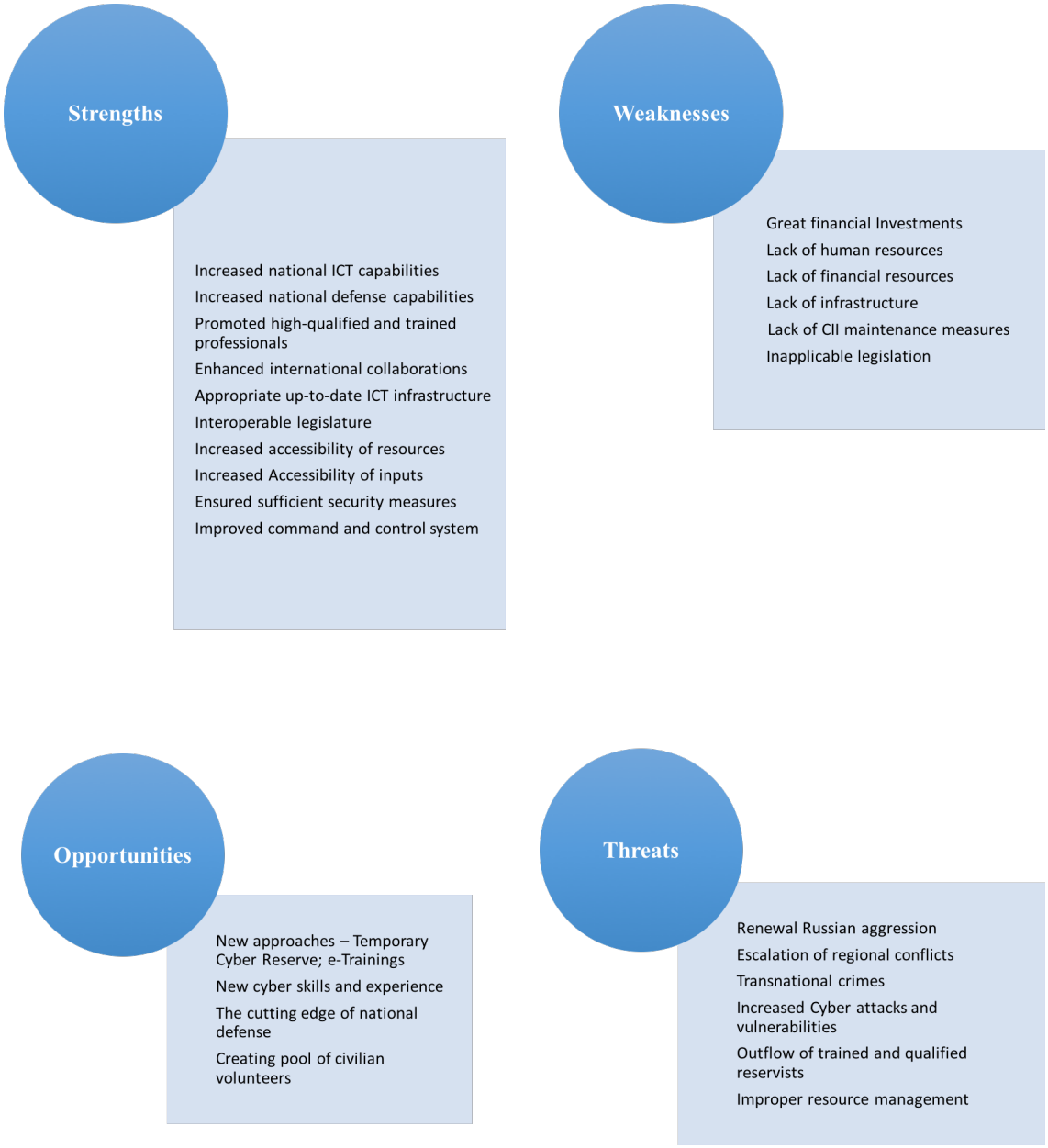
security procedures and tool to ensure the confidentiality of ICT infrastructure and development of confidence into e-services. To achieve desirable goals security technologies should be user friendly, transparent, cost effective, third party controllable and auditable.

- ***Social dimension***

  In order to get sufficient level of awareness among information society, any citizen should understand the significance of vulnerabilities and their impacts for the end-users. Thus they should understand how to implement and develop global cybersecurity culture based on well recognized international standards and competence. Moreover, these goals will not be achieved without high-educated manpower in these fields. The education is a cornerstone and key factor to become an honourable member of information society. it is only weapon to cope with vulnerabilities and threats existing in digital world, and to enhance confidence and security in the use of ICT [11] .

SWOT Analysis

Table 3. SWOT Analysis of creating additional national security unit



4.2 Proposals, Requirements, Constraints

In the final section, it will be assumed the possible cyber defense approaches for Georgia based on international experiences and well practice. Possible limitations and necessary steps for each solution will be analyzed as well, which will allow to make final recommendations, well tailored to the Georgia's example. Furthermore, by

transferring and sharing knowledge and experience for other small and developing countries will help them to find their own good practices. The following approaches should be fruitful and should be done in such manner that they become driving force for economy and the results are reflected in economic prosperity.

There is no doubt that the war in 2008 was a great shaker for Georgia in security development contest. Although its reaction did not get as high-resolution as Estonia put in 2007, from today's perspective, in these eight years it has prepared fundament for future developments and significant changes to build on it. Even if we can discuss today on cyber capacity building of Georgia and its future capabilities it means that there is a will and readiness for better, more secure, transparent and prosperous future on governmental level, either from society side.

The previous chapters are explicit proof of the fact that Georgia needs to develop proper cyber security policy and to make it operable which will ensure sustainability and security in the country. The Country's position must be expressed precisely. Georgia doesn't seek offensive capabilities, rather it should be focused on defensive capabilities.

Due to the internal and foreign developing trends of using ICT tools in every field of economy and increasing opportunities for cyber threats, an establishment and development of cyber security reserve unit is urge for the country. The thesis is dedicated to elaborate the institutional structure of cyber reserve, which will be responsible for ensuring secure, sustainable and high-tech environment. In these complex socio-technical systems, which are continuously evolving, the unit will ensure defense oriented activities and all necessary measures to prevent potential threats and vulnerabilities.

Beside the situation of several years ago, when there was not any governmental unit, which would be responsible for cyber threats and vulnerabilities and secure the society, nowadays their number has increased significantly. The Data Exchange Agency, the Cyber Security Bureau, CERT.GOV.GE, CSIRT/CC, State Security Service and et al. are clear declaration of this.

On the one hand, an additional security institute will strengthen the forces to get the main goals: transparency, accountability and integrity in international institutions. These will be achieved based on several conditions:

- Improved command and control systems
- Effective planning and execution
- Developed critical defense capabilities
- Improved resource management
- Established modern educational, training and personnel management systems
- Conducted scenario-based exercises and combat trainings
- Enhanced NATO interoperability

On the other hand, there should be defined its responsibilities and functions very accurately and clearly to get effective and operable mobilizing system. Thus, it will represent an auxiliary detachment of other cyber forces for government to control and defense national cyberspace. It should neither overlap the functions of other cyber security institutes, nor should create the additional problems in its own cyberspace.

To take into account international experience and well practice of above mentioned examples, there are two choices – mandatory cyber reserve or voluntary cyber reserve as it is in most developed countries. All three above discussed examples show that the reserve is preferred to be based on optional principles. To get the desired consequences it should be the choice and declaration of will to take part in building national security capabilities and strengthening defense of national cyberspace. To get higher contribution, everyone has the right to make a choice which will be guarantee against the detrimental consequences.

Based of the past experience what happened in Estonia in 2007, and in Georgia in 2008, we can assume that the cyber reserve mobilization will be necessary when government can not attract enough technological expertise to protect the pubic interest. It should be mentioned that in reasonable frames, cyber conscription system will be able to plan in advance which means that it will be implemented before cyber attacks occur or are expected to occur. Cyber conscription, in other words, would allow the governments to obtain the proactive services of IT specialists which may decline to assist in urgent situations because they would get more benefits from private employment.

Some military leaders claim that existing cultures of the Army, Navy, and Air Force are fundamentally incompatible with that of cyber warfare. For these and other reasons, we believe that the appropriate model for cyber reserve is proactive mobilization based on

voluntary principles. From this facets, cyber reserve forces will be formed and trained before needs arise and will be conscripted to activate service when the need arises.

Since the cyber attacks are characterized with the inherent ambiguity from the scope of the intent, duration, sources and cyber attackers operate with different aims from different locations, it puts forward the issue of required criteria for calling up and activating cyber reserve. Based on the examples of the military forces which are not allowed to interfere in the local forces/police cases, the same argument can be used for cyber reserve. For instance, if police need help and can not handle to the existed public disorder then the decision to add additional resources and activate the national defense forces is justified. Using the similar approach, it may be suggested that the cyber reserve should not be activated if there is no clear evidence of cyber attacks occurring or are expected to occur and it will not create vulnerabilities for national cyberspace, national critical information infrastructure or for human life. The clear example of these are attacks on power grid, medical facilities or water supplies. Additionally, objective activation of the cyber reserve will obtain the effective serving of cyber defense forces.

As it is known, Georgia is one of the post-Soviet countries, which still remains the footsteps left from the past. Thus, this small developing country tries to cope with overarching responsibilities with very limited resources. Historically, calling up in reserve has been levy in mass or kind a fortune's wheel, which was related to the question - to be or not to be. It was caused by inevitable consequences, sacrificing innocent lives of conscripts in most cases, which scattered the encouragement and patriotic doughtiness. The kinetic wars, waged with physically present on the targeted state's territory to carry out attacks or defensive activities, were prolonged because they were zero-sum battle to achieve the certain goals.

However, cyber warfare is waged remotely, which ensures decreasing the risk that cyber attacks will disrupt the lives of conscripts physically. Until recently, if in the past wars the massed manpower was crucial and predominant engine to perform particular results, things changed and cyber warfare anginas are very different. Targeted selection of proper manpower with specialized talents and skills plays an important role in cyber reserve operability. Collecting IT staff requires very careful selection based on detailed information about working experience and education background, including the knowledge level of industries, various platforms and software. Based on this approach,

it is not necessary the physical fitness to be able to conduct cyber operations, rather than recruit people for their thinking and cyber-cognitive abilities. It calls for government to put more effort and plan more accurately the selection process and for potential reservists to take responsibility more seriously. Only such selected and structured reserve can be competitive and equitable.

According to Estonian researcher, Martin Hurt who evaluated national defense strategy and readiness of Estonia, assumed that Estonia needs to improve the quality not quantity of the forces. This assumption also very suitable for Georgia's example. There is a need more specifically forces which are able to respond and react on time. [97]

The lack of expertise and manpower can be a major obstacle for the government to meet the climbing demand of cyber-security preparedness. On the other hand, it will be responded with wider selection of suitable candidates in terms of sex, physically discarded people for military armed forces, increased scale of age. This approach also responds the global issue like gender equality. The number of females involved in ICT sectors are increasing, which allows to premise that the females also express the interest to joint cyber forces and serve for the national cyberspace defense. Moreover, it opens the another opportunity for people with disability or people who were excluded under the previous rules. The presumption that there is no need for defining the upper limit of the age emphasizes the capabilities of the project to attract the wide spectrum of society.

In order to attract the people who may not have had desire to volunteer or could not have been considered in the past, the eligibility criteria should be flexible as much as possible. The primary criteria for applying to serve in Cyber Reserve might be the following:

- Being citizen and lived in state for more than 10 years
- Having required cyber skills
- Satisfying desirable qualifications
- Being able to attend on the regular trainings
- Being of the full legal age (more that 18 years old)
- Being able to support cyber security missions

The optimized allocation of human resources is one of the cornerstone in this contribution as well as contract period of serving. Here, it can be utilized article 4 of the Third Geneva Convention, under which members of cyber reserve [120] :

- Will become combatants when they are called to duty
- Will otherwise occupy the status of civilian non-combatants

In this regard, the international competences offer two options of activation period for cyber reserve – permanent or temporary duty. The permanent serving period means that cyber reservists will be full-time member of military and permanently in duty. This option excludes serving of cyber reservists under their civilian status, which means that they will unable to get civilian employment. Furthermore, countries that will elect this option automatically appropriates the essential high-qualified and trained IT professionals from other sectors, which arises the counterproductive situations for the development of the country.

On the other hand, second option is temporary cyber reserve, which includes the situational activation of cyber forces. In other words, calling up for duty will continue as long as attacks or threat of attack exist. Otherwise, when this special regime ends, the cyber reservists will be relieved from the duty and returned to their civilian status.

To discuss these two models in terms of costs and benefits, the situational activation model has the comparative advantage because there is no need and significant benefits from permanent serving model, especially when high-qualified and trained professionals in IT fields can be more productive and bring more benefits in both civilian and non-civilian duty. There is also another point of the temporary cyber duty, the length of reserve contracts – how long the reservists should be under the status of reservist. As security experts suggests, the reasonable time for the serving period under the same contract is five years. This is the maximum period, among which changes of conditions remains same consequences. A longer period is not recommended because of fast pace of technological changes and/or an incompatibility of the reservist's qualification which was suitable five years before.

Discussing cyber reserve contract, compensation during serving period also should be considered. It should be defined in a reasonable way under the Georgian legislation. Along serving period, reservist take significant responsibilities in front of public and

private employment as well. They would not want to take additional responsibilities without adequate compensation while as they are high professionals there is always high demand from different private sectors and can hold more than one office. However, for the government, there is always exist inherent risk of termination the contract before the expired time and staff outflow, which means that investments in training and transactions may be wasted. This topic should be regulated with reserve employment contract under the law on cyber reserve.

4.2.1 e-Training

One of the main components of our suggestions under the Cyber Reserve Program is e-training, which means applying e-learning tools to military distance learning. As it was already mentioned, besides the fact that modern ICT tools increase vulnerabilities and threats, they also bring the number of opportunities and advantages. Among them are e-leaning tools from e-service family. Web-based cyber solders trainings will allow the government to save the time and financial costs, to ensure the auspicious conditions for cyber reservist more productive on their jobs, and to create new working places and trends in modern education system.

According to Besser and Bonn, 1977, some great success stories in the early paradigms of distance learning come from the field of training, not education [104] . A challenge is to channel and rapport the natural interests in organizational communities into training and learning communities that can enhance the development of skills and acquisition of knowledge by soldiers. To establish and develop this kind of learning community there are several elements which should be considered:

- Identity element
- Participation element
- Integration element
- Feedback element

These principles should be of concern to those involved with the shift from a classroom training model to a soldier-centric model of training. This approach will allow cyber reservists to take part in all training and accomplish their training sessions fully, practice at their own convenience and at a pace that is right for them. Thus, they will be able to

work in distance and be more productive on privet jobs as well as in cyber reserve serving.

To establish this approach, it calls for government to ensure several bases:

- Appropriate ICT infrastructure
- Suitable and adopted software
- Sufficient security measures
- Suitable Legal framework
- Justified Regulatory framework
- Appropriate guidelines and curriculum
- Qualified coaches and trainers

On the other hand, for potential reservists it will be hugely attractive to receive cyber skills and experience at the cutting edge of national defense. We believe that time after time it become very popular and at the same time very prestigious to serve in national cyber reserve and get the status of national cyber reservist. In the future the status even become guarantee of the quality which means that after closing the contract and serving in the public reserve it will open other opportunities to the reservists. Creating the pool of civilian professional volunteers in public sector will exert the influence over economic growth and innovation.

5 Conclusion and Future Work

5.1 Summery of Findings

This paper shows that though cyber security is contingent on a variety of factors that vary by country, Georgia can best position themselves for future improvement by focusing policy on areas that improve technological, social, and economic outcomes to benefit the state. The aim of this work was to reveal the main problems in current ICT sectors of Georgia, which are densely networked to national security and defense of cyberspace of the country, to identify threats and vulnerabilities, to examine the international experience of countries with similar problems and find the best solutions based on well practices. Moreover, to suggest the operable model of cyber defense unit which will ensure effective and fruitful inter-agency cooperation and integration with international unions and standards.

Increasing number of threats and vulnerabilities in our environment, brings us to mobilizing IT specialists under the cyber reserve system as an additional cyber unit of national armed forces. This solution is a direct consequence of the discussion that cyber security addresses the defense of society as a whole and requires the whole of government integrated approach. From this scope of view, our recommendations rely on the complex approach which enables government to ensure high security level of society. As we already mentioned in the previous paragraph, the separate improvements in information infrastructure without enforcements in legislation and education system will not bring the desirable results. It is important to push changes in these components simultaneously.

The solutions and recommendations distributed through this thesis are based on international experience and competences. I explore the examples of the US Cyber Command, UK Joint Cyber Unit (Reserve) and Estonian Cyber Defense League in order to make final proposals applicable for Georgia. These three countries have already used the cyber reserve approach to strengthen their national security and defense national cyberspace successfully. Their success is measured and expressed in different kind of

international indexes like e-participation, e-governance development and networked readiness indexes, which evaluate their performance among many other countries. We believe that our suggestions will also help to Georgia to improve its positions and go forward to achieve higher positions on international level.

Additional innovative component of our research paper is e-training model based on e-learning tools which will allow the government to save the time and financial costs significantly. It will be also convenient for potential reservists and their civilian employers because they will be able to be more productive on their jobs.

My ultimate conclusion is that addition cyber security unit like cyber reserve offer a great opportunity to strengthen cyber capabilities of the country which in long term will be reflected in economic growth and prosperity.

5.2 Future Work

Although the solutions presented in this thesis have demonstrated the significance and effectiveness of National Cyber Reserve of Georgia, it could be developed in number of different ways. Further search for Cyber Reserve establishment and development forms for other small and developing countries would be advanced and preferable to understand all potential benefits and a role of the cyber reserve system in economic development and prosperity. Thus, to find other time and cost-effective ways to implement and develop cyber reserve training, beside the e-training platform, would be interesting and considerable contribution for further action-design research paper [122] Since cyberspace became a specific domain for countries and as they pay more attention cyber related issues more empirical data will allow to them to open the ICT doors wider.

References

[1] Runeson, P. and Höst, M., 2009. Guidelines for conducting and reporting case study research in software engineering. Empirical software engineering, 14(2), pp.131-164.

[2] Salim, H.M., 2014. Cyber safety: A systems thinking and systems theory approach to managing cyber security risks (Doctoral dissertation, Massachusetts Institute of Technology).

[3] Siponen, M. and Willison, R., 2009. Information security management standards: Problems and solutions. Information & Management, 46(5), pp.267-270.

[4] Von Solms, B. and Von Solms, R., 2004. The 10 deadly sins of information security management. Computers & Security, 23(5), pp.371-376.

[5] Cybersecurity, C.I., 2014. Framework for Improving Critical Infrastructure Cybersecurity.

[6] Burt, D., Nicholas, K.S., Sullivan, K. and Scoles, T., 2014. The cybersecurity risk paradox: impact of social, economic, and technological factors on rates of malware. Microsoft Security Intelligence Report Special Edition (SIR), Microsoft Corporation.

[7] McQueen, M.A., Boyer, W.F., Flynn, M.A. and Beitel, G.A., 2006, January. Quantitative cyber risk reduction estimation methodology for a small SCADA control system. In System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on (Vol. 9, pp. 226-226). IEEE.

[8] McGlinchey, E. and Johnson, E., 2007. Aiding the Internet in central Asia. Democratisation, 14(2), pp.273-288.

[9] Dyer-Witheford, N., 1999. Cyber-Marx: Cycles and circuits of struggle in high-technology capitalism. University of Illinois Press.

[10] Cybersecurity Policy Making at a Turning Point. (2012). OECD Digital Economy Papers.

[11] Schjølberg, S. and Ghernaouti-Hélie, S., 2009. A global protocol on cybersecurity and cybercrime. Cybercrimelaw. net.

[12] Berry, J.W., 2006. The World Summit on the Information Society (WSIS): A global challenge in the new Millennium. Libri, 56(1), pp.1-15.

[13] "The World Summit on the Information Society (WSIS): TUNIS AGENDA FOR THE INFORMATION SOCIETY, 2005. Retrieved from http://www.coe.int/t/dgap/goodgovernance/Activities/Public_participation_internet_governance/tunis_agenda.official_en.asp"

[14] Pilling, R., 2013. Global threats, cyber-security nightmares and how to protect against them. Computer Fraud & Security, 2013(9), pp.14-18.

[15] Grove, G.D., Goodman, S.E. and Lukasik, S.J., 2000. Cyber-attacks and. Survival, 42(3), pp.89-103.

[16] Aslanoglu, R. and Tekir, S., 2012, July. Recent Cyberwar Spectrum and its Analysis. In European Conference on Information Warfare and Security (p. 45). Academic Conferences International Limited.

[17] ალექსანდრე ღლონტი, 2013. კიბერდანაშაულის პრობლემა საქართველოსა და უცხოეთის ქვეყნებში. GRIGOL ROBAKIDZE UNIVERSITY ACADEMIC DIGEST BUSINESS AND MANAGEMENT (SPECIAL EDITION), (1), pp.37-45.

[18] Georgia - ICT Development - Harmonisation of Laws and Acceleration of Broadband Roll-out. Retrieved April 5, 2016, from http://www.ebrd.com/work-with-us/procurement/pn-48769.html

[19] ICT COUNTRY PROFILE GEORGIA_USAID, 2013. Retrieved from http://www.rciproject.com/itprofiles_files/ICT%20Country%20Profile%20Georgia_2013_1.0.pdf

[20] Czosseck, C., Ottis, R. and Talihärm, A.M., 2013. Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. Case Studies in Information Warfare and Security for Researchers, Teachers and Students, p.72.

[21] Georgia. (2010). Retrieved from https://opennet.net/research/profiles/georgia

[22] MSHVIDOBADZE, K., 2015. GEORGIA CYBER BAROMETER REPORT.

[23] A Digital Georgia. (2015). Retrieved from http://www.dea.gov.ge/uploads/egeorgia strategy.pdf. e-Georgia strategy and action plan 2014-2018.the framework of Component 4 of the twinning project "Promote the strengthening of E-Governance in Georgia (E-Government Georgia)"

[24] Jackson, E.B., Open Georgia: How Open Data Can Be Used As An Anti-Corruption Tool.

[25] T. I. T. T., & T. T. 2014, August. Internet Freedom in Georgia – Report N3-4. Retrieved from https://idfi.ge/en/internet-freedom-in-georgia-report-n3-4

[26] 2014 Annual Report. (2014). Tbilisi: საქართველოს კომუნიკაციების ეროვნული კომისია

[27] World Economic Forum; The Global Information Technology Report 2015; Date of data collection or release: 15th April 2015; www.weforum.org/gitr

[28] Internet Usage and Population Statistics Retrieved from http://www.internetworldstats.com/asia/ge.htm

[29] Network Readiness Index retrieved from http://www3.weforum.org/docs/WEF_Georgia.pdf

[30] The Global Information Technology Report 2015 retrieved from http://www3.weforum.org/docs/WEF_GITR2015.pdf

[31] CRRC (Caucasus Research Resource Centers). (2015). Comparing civic participation: Caucasus Data 2007. Social Science in the Caucasus [blog] (May,2015). Available at: http://crrc-caucasus.blogspot.com/2015/08/internet-and-social-media-usage-in.html

[32] United Nations Department of Economic and Social Affairs (UNDESA), UN E-Government Development Database (retrieved November 27, 2014)

[33] e-governance development index, 2015, retrieved from https://publicadministration.un.org/egovkb/en-us/Data/Compare-Countries

[34] Thornton, Laura, Public Attitudes in Georgia. National Democratic Institute, 2014. Undated. Retrieved from https://www.ndi.org/files/NDI_Georgia_August-2014-survey_Public-Issues_ENG_vf.pdf

[35] Statistics of Facebook users, 2015. Retrieved from http://www.katypearce.net/january-2015-facebook-use-in-armenia-azerbaijan-and-georgia-according-to-facebook/

[36] Law of Georgia of Information Security. Retrieved from https://matsne.gov.ge/en/document/download/1679424/3/en/pdf

[37] Governmental Order #312 on approval of the critical information system subjects list. Legislative Herald of Georgia, April 29, 2014. Retrieved from http://gov.ge/files/382_41998_391311_312290414.pdf

[38] Governmental Order #567 on approval of the critical information system subjects list in Defense eld. Legislative Herald of Georgia. September 29, 2014. Retrieved from https://matsne.gov.ge/ka/document/view/2521602"

[39] Law on Criminal Procedure Code. Amendments to the Law on Criminal Procedure Code. Legislative Herald of Georgia. November 30, 2014. Retrieved from https://matsne.gov.ge/en/document/view/16426

[40] GDP of Georgia. Retrieved from http://www.tradingeconomics.com/georgia/indicators

[41] ISPs of Georgia. Retrieved from http://analytics.gncc.ge/en/statistics/?c=internet&f=subscribers&exp=technologies&sid=112631#

[42] State Security and Crisis Management Counsel. Retrieved from https://www.matsne.gov.ge/ka/document/view/2186268

[43] Primer Minister comment regarding to merging. Retrieved from http://newsday.ge/new/index.php/en/component/k2/item/14721-the-pm-in-state-security-and-crisis-management-council

[44] Ministry of Internal Affairs. Retrieved from http://police.ge/ge/projects/kiberdanashauli/shinagan-saqmeta-saministros-mier-gankhortsielebuli-ghonisdziebebi

[45] Ministry of Defence. Ministry's Vision. Retrieved from 2015-2016https://mod.gov.ge/assets/up-modul/uploads/pdf/Ministers-Vision-Geo.pdf

[46] Georgian ICT Development and Cyber Security Event. Retrieved from http://www.ictbc.ge/?17/

[47] 2014 Annual Report. Data Exchange Agency. Undated. Retrieved from http://www.dea.gov.ge/uploads/DEA_Anual_report_2014_Draft_v1_2.pdf

[48] Mobile Application. Newsletter of Data Exchange Agency, January, 2016. Retrieved from http://dea.gov.ge/uploads/NEWSLETTER_January_2016_GEO.pdf

[49] Trade Facility Systems. Newsletter of Data Exchange Agency, January, 2016. Retrieved from http://dea.gov.ge/uploads/NEWSLETTER_October%202015_GEO.PDF

[50] Georgia 2020. Ministry of Economy and Sustainable Development of Georgia. Retrieved from http://www.adb.org/sites/default/files/linked-documents/cps-geo-2014-2018-sd-01.pdf

[51] Techno Park. Ministry of Economy and Sustainable Development of Georgia. Retrieved from http://techpark.ge/Techpark.pdf

[52] Swanson, L., 2010. Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict, The. Loy. LA Int'l & Comp. L. Rev., 32, p.303.

[53] Klimburg, A., 2011. Mobilising cyber power. Survival, 53(1), pp.41-60.

[54] Kiely, L. and Benzel, T.V., 2006. Systemic security management. Security & Privacy, IEEE, 4(6), pp.74-77.

[55] Potter, J. and Ruhlman, M., 2010. cooking for geeks. O'Reilly Media, Incorporated.

[56] Shakarian, P., 2011. The 2008 Russian Cyber Campaign Against Georgia. Military Review, 91(6), p.63.

[57] Hollis, D.M., 2011. Cyberwar case study: Georgia 2008. Journal Article| January, 6(11).

[58] Cyber Security Strategy of Georgia 2012-2015, from http://www.dea.gov.ge/uploads/National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf

[59] "THE USE OF THE INTERNET FOR TERRORIST PURPOSES. Retrived from https://www.coe.int/t/dlapil/codexter/Source/cyberterrorism/Georgia.pdf"

[60] Korns, S.W. and Kastenberg, J.E., 2008. Georgia's cyber left hook. Parameters, 38(4), p.60.

[61] Army Reserve Quarterly. 2014. Sign up for Cyber. Retrieved March 22, from http://www.army.mod.uk/documents/general/ADR003024_ARQ_21_web.pdf

[62] "BBC News. 2012. UK planning the Cyber Reserve Defense Force. Retrieved March 22, from http://www.bbc.com/news/uk-politics-20578691"

[63] Cabinet Office. 2014. The UK Cyber Security Strategy: Report on Progress and Forward Plans. Retrieved March 22, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf

[64] Coller, J. 2015. A British Cyber Defense League. Retrieved March 22, from http://www.ccw.ox.ac.uk/blog/2015/11/26/a-british-cyber-defence-league

[65] Defense Academy of the United Kingdom. (n.d.). About the Defense Academy of the United Kingdom. Retrieved March 22, from http://www.da.mod.uk/about-us

[66] Joint Forces Command. (n.d.a) About us. Retrieved March 22, from https://www.gov.uk/government/organisations/joint-forces-command/about

[67] Joint Forces Command. (n.d.b) The Permanent Joint Headquarters. Retrieved March 22, from https://www.gov.uk/government/groups/the-permanent-joint-headquarters

[68] Joint Forces Command. (n.d.c). Directorate of Special Forces. Retrieved March 22, from https://www.gov.uk/government/groups/defence-intelligence

[69] Joint Forces Command. (n.d.d). Defense Intelligence. Retrieved March 22, from https://www.gov.uk/government/groups/defense-intelligence

[70] Joint Forces Command. (n.d.e) Defense Medical Services. Retrieved March22, from https://www.gov.uk/government/groups/defence-medical-services

[71] Ministry of Defense. 2012. Permanent Joint Operating Bases (PJOBs). Retrieved March 22, from https://www.gov.uk/government/publications/permanent-joint-operating-bases-pjobs/permanent-joint-operating-bases-pjobs

[72] Dandeker, C., Greenberg, N. and Orme, G., 2011. The UK's reserve forces: retrospect and prospect. Armed Forces & Society, 37(2), pp.341-360.

[73] Hannan, N.K., 2015. Use of Reserve Forces in Support of Cyber-Resilience for Critical National Infrastructure: US and UK Approaches. The RUSI Journal, 160(5), pp.46-51.

[74] Tinker, P.W., 2015. For the Common Defense of Cyberspace: Implications of a US Cyber Militia on Department of Defense Cyber Operations. ARMY COMMAND AND GENERAL STAFF COLLEGE FORT LEAVENWORTH KS.

[75] Aucsmith, D. 2015, June. Implications of Cyber Warfare. In Proceedings of 3rd ACM Workshop on Information Hiding and Multimedia Security (pp. 1-1). ACM.

[76] Heitel, S., Kämpf-Dern, A. and Pfnür, A., 2015. Integration of stakeholder interests in housing companies' strategic management: A process model for more sustainable value creation. Property Management, 33(3), pp.224-244.

[77] Iramacami, T. (2010). Principles of management. Mumbai [India]: Himalaya Pub. House.

[78] Karadağ, B., Ikitimur, B. and Ongen, Z., 2012. [Perioperative management in patients receiving newer oral anticoagulant and antiaggregant agents]. Turk Kardiyoloji Dernegi arsivi: Turk Kardiyoloji Derneginin yayin organidir, 40(6), pp.548-551.

[79] Laudon, K.C. and Laudon, J.P., 2004. Management information systems: managing the digital firm. New Jersey, 8.

[80] Maney. K, Hamm, S. and O'Brien, J. (2011). Making the work better. Upper Saddle River, NJ: IBM Press

[81] Parker, T., Sachs, M., Shaw, E. and Stroz, E., 2004. Cyber adversary characterization: Auditing the hacker mind. Syngress.

[82] Protect your workplace, guidance on physical and cyber security and reporting of suspicious behavior, activity, and cyber incidents. (2006). [Washington, D.C.]: United States Dept. of Homeland security.

[83] Quiggin, T. (2012). Don't call us. Kingston, Ont.: Centre for International and Defense Police, Queen's University.

[84] Drennan, L. and Rejda, G.E., 2003. Principles of Risk Management and Insurance. Risk Management, 5(3), pp.65-65.

[85] Vaseashta, A., Susmann, P. and Braman, E. eds., 2014. Cyber Security and Resiliency Policy Framework. IOS Press.

[86] Duklis Jr, P.S., 2002. The Joint Reserve Component Virtual Information Operations Organization (JRVIO); Cyber Warriors Just a Click Away. ARMY WAR COLL CARLISLE BARRACKS PA.

[87] Czosseck, C., Ottis, R. and Talihärm, A.M., 2013. Estonia after the 2007 cyber attacks: Legal, strategic and organisational changes in cyber security. Case Studies in Information Warfare and Security for Researchers, Teachers and Students, p.72.

[88] Kaska, K., Osula, A., Stinissien, J. (2013). The Cyber Defense Unit of the Estonian Defense League: Legal Policy and Organizational Analysis. Tallin: CCDCE

[89] 2014-2017 Cyber Security Strategy of Estonia (2014). Retrieved from https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf

[90] The Defense League Act (2013), Retrieved from https://www.riigiteataja.ee/en/eli/525112013006/consolide

[91] NATO Cooperative Cyber Defense Centre of Excellence. Retrived from https://ccdcoe.org/history.html

[92] Estonian Defence League's Cyber Unit. Retrieved from http://www.kaitseliit.ee/en/cyber-unit

[93] ვაჟა გურაბანიძე, 2013. ადამიანური რესურსების სტრატეგიული მენეჯმენტი და მისი რეალიზაცია. JOURNAL" ECONOMIC PROFILE" KUTAISI UNIVERSITY, (12), pp.37-40.

[94] Tammet, T., Volunteers and Cyber Security: Options for Georgia.

[95] Hollis, D.M., 2011. A Reserve Component Initiative to Defend DoD and National Cyberspace. OFFICE OF THE UNDER SECRETARY OF DEFENSE

(INTELLIGENCE) WASHINGTON DC CYBERSPACE WARFIGHTER INTEGRATON AND STRATEGIC ENGAGEMENT DIV.

[96] Savvides, A., Paschalidis, I. and Caramanis, M., 2011. Cyber-physical systems for next generation intelligent buildings. ACM SIGBED Review, 8(2), pp.35-38.

[97] Crandall, M., 2014 Mandatory Military Service and Small European States: Ready to Fight Yesterday's Battles.

[98] Dandeker, C., Greenberg, N. and Orme, G., 2011. The UK's reserve forces: retrospect and prospect. Armed Forces & Society, 37(2), pp.341-360.

[99] NewsDayGeorgia: Discussions on Mobilization and Reserve Draft Concept with MPs http://newsday.ge/new/index.php/en/component/k2/item/18090-discussions-on-mobilization-and-reserve-draft-concept-with-mps

[100] Strategic Defence Review of Georgia 2013-2016. Retrieved from http://www.mod.gov.ge/assets/up-modul/uploads/pdf/SDR-ENG.pdf

[101] Brenner, S.W. and Clarke, L.L., 2011, June. Conscription and cyber conflict: Legal issues. In Cyber Conflict (ICCC), 2011 3rd International Conference on (pp. 1-12). IEEE.

[102] რეზერვის ახალი კონცეფცია, რომელიც სავალდებულო სამხედრო სამსახურთან ერთად იმოქმედებს, April, 2016. Retrieved from http://netgazeti.ge/news/103479/

[103] Protocol, I., 1977. Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts. Opened for signature on, 12.

[104] Bonk, C.J. and Wisher, R.A., 2000. Applying collaborative and e-learning tools to military distance learning: A research framework. ARMY RESEARCH INST FOR THE BEHAVIORAL AND SOCIAL SCIENCES ALEXANDRIA VA.

[105] Rjaibi, N., Rabai, L.B.A., Aissa, A.B. and Louadi, M., 2012. Cyber security measurement in depth for e-learning systems. International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 2(11), pp.107-120.

[106] Prensky, M. and Prensky, M., 2007. Digital game-based learning (Vol. 1). St. Paul, MN: Paragon house.

[107] Social-economic Development Strategy of Georgia "GEORGIA 2020", retrieved from http://www.adb.org/sites/default/files/linked-documents/cps-geo-2014-2018-sd-01.pdf

[108] LELP Cyber Security Bureau, 2016. Retrieved from http://csbd.gov.ge/bureau.php?lang=en

[109] Ministry of Justice of Georgia, 2016. Retrieved from http://www.justice.gov.ge/Ministry/Index/383

[110] Georgian ICT Development and Cyber Security Event, GITI 2015. Retrieved from file:///Users/TamarTatuTabagari/Documents/TUT%202015:III%20Semester/Master's%20Thesis/Reading%20Materials/Georgia_ICT%20Background/GITI%202015%20%20%20Georgian%20ICT%20Development%20And%20Cyber%20Security%20Event.webarchive

[111] LELP Smart Logic, Georgia. 2016. Retrieved from http://www.opendata.ge/en/institutions/639

[112] LELP Data Exchange Agency, Ministry of Justice. 2016. Retrieved from http://www.dea.gov.ge/?action=page&p_id=5&lang=geo

[113] My.gov.ge, 2016. Retrieved from https://www.my.gov.ge/public/home/index?id=22&type=Main&index=0&p1=22

[114] LELP National Agency of Public Registry of Ministry of Justice. Retrived from https://napr.gov.ge/m/0

[115] CERT.GOV.GE, retrieved from http://www.cert.gov.ge

[116] Ministry of Economy and Sustainable Development. Retrieved from http://www.economy.ge

[117] Bērziņš, J., 2014. Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy. National Defence Academy of Latvia Center for Security and Strategic Research. Policy Paper, (2), pp.2002-2014.

[118] Crandall, M., Mandatory Military Service and Small European States: Ready to Fight Yesterday's Battles.

[119] Gov.uk. 2011. The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. Retrieved March 22, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

[120] Pictet, J.S. and De Preux, J., 1960. GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR.

[121] Shenton, A.K., 2004. Strategies for ensuring trustworthiness in qualitative research projects. Education for information, 22(2), pp.63-75.

[122] Sein, M., Henfridsson, O., Purao, S., Rossi, M. and Lindgren, R., 2011. Action design research.

Appendices

Appendix 1 – The list of Critical Information Infrastructure

Administration of the President

Parliament of Georgia

Ministry of Economy and Sustainable Development

Ministry of Labour, Health and Social Affairs

Ministry of Development and Infrastructure

Ministry of Internal Affairs

Ministry of Finance

Ministry of Foreign Affairs

Ministry of Corrections

Ministry of Justice

State Service Development Agency, LEPL

National Examination Center, LEPL

Social Service Agency, LEPL

State Procurement Agency, LEPL

Smart Logic, LEPL

The Central Election Commission

Tbilisi City Hall

The Office of Chief Prosecutor of Georgia

National Bank

Government Chancellery

Land Transport Agency, LEPL

Maritime Transport Agency, LEPL

Civil Aviation Agency, LEPL

Georgia Health Mediation Service, LEPL

National Center for Diseases Control and Public Health, LEPL

State Regulatory Agency for Medical Activities, LEPL

Financial Monitoring of Georgia, LEPL

Revenue Service, LEPL

National Civil Registry Agency, LEPL

Financial and Analytical Service, LEPL

Education Management Information System, LEPL

Georgian Railway, JSC

Sakaeronavigatsia, LTD (Air Traffic Control)

United Airports of Georgia, LTD

National Center for Education Quality Enhancement, LEPL

Border Police, MIA

Service Agency MIA, LEPL

Service of “112” MIA, LEP

National Environment Agency, LEPL

Appendix 2 – The State Cyber Security Management Chart