TALLINN UNIVERSITY OF TECHNOLOGY

Department of Software Science

School of Information Technology

ITC70LT

Javid Asadli 165601IVCM

PROPOSING ACTION PLAN IN CYBER SECURITY CAPACITY BUILDING FOR AZERBAIJAN

Master Thesis

Tiia Sõmer, MSc

Tallinn University of Technology

Leyla Aliyeva, MSc

CERT Azerbaijan

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: Javid Asadli

Abstract

Increasing effect of cyber security in national level requires to improve and develop national cyber security capacity programs. Cyber security capacity building includes itself all areas of cyber security to develop country in that manner. In this research five main dimensions have been considered and existing situation regarding cyber security capacity building in the Azerbaijan Republic was investigated. The author analyzed the current situation by investigating local documents and conducting a survey of IT and Cyber Security experts. At the end of the thesis, an action plan has been proposed to improve challenges in cyber security capacity building in Azerbaijan.

This thesis is written in English and is 81 pages long, including 5 chapters, 31 figures and 8 tables.

Abstract Estonian

Küberjulgeoleku üha suurenev mõju riiklikul tasandil nõuab riiklike küberjulgeoleku suutlikkuse programmide täiustamist ja arendamist. Küberjulgeoleku suutlikkuse suurendamine hõlmab ise kõiki küberjulgeoleku valdkondi, et sellisel viisil riiki arendada. Käesolevas uuringus on käsitletud viit peamist mõõdet ning täpsemalt uuriti Aserbaidžaani Vabariigi küberjulgeoleku suutlikkuse tõstmisega seotud hetkeolukorda. Autor analüüsis praegust olukorda, uurides riiklikke dokumente ja viies läbi uuringu infotehnoloogia ja küberjulgeoleku ekspertide seas. Väitekirja lõpus on esitatud Aserbaidžaani küberjulgeoleku suutlikkuse suurendamise väljakutsetega seotud tegevuskava.

Käesolev väitekiri on inglise keelne ja 81 lehekülge pikk, sealhulgas 5 peatükki, 31 joonist ja 8 tabelit.

Table of abbreviations and terms

AzStand	State Committee for Standardization, Metrology and Patents of The Republic of Azerbaijan
CC	Criminal Code
CCDCOE	Cooperative Cyber Defense Center of Excellence
CERT	Computer Emergency Response Team
CERT.AZ	National Computer Emergency Response Team of Azerbaijan
CI	Critical Infrastructure
CSOC	Cyber Security Operations Center
CSCB	Cyber Security Capacity Building
CoE	Council of Europe
CIS	Commonwealth of Independent States
EE	Estonia
EU	European Union
FIRST	Forum of Incident Response and Security Teams
GCSI	Global Cyber Index
GCVI	Global Cyber Vulnerability Index
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
ICT	Information Communication Technologies
IoT	Internet of Things

ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISP	Internet Service Providers
IT	Information Technologies
ITU	International Telecommunication Union
MinCom	Ministry of Transport, Communications and High Technologies
MIA	Ministry of Internal Affairs
MoD	Ministry of Defense
NATO	North Atlantic Treaty Organization
OECD	Organization for Security and Cooperation in Europe
OIC-CERT	Organization of The Islamic Cooperation - Computer Emergency Response Teams
OS	Operation System
OSCE	Organization for Security and Cooperation in Europe
PPP	Public-Private Partnership
R&D	Research and Development
RI	Random Index
SSPS	Special State Protection Service
SSS	State Security Service
SME	Small and Medium-sized Enterprises
UN	United Nations

Table of Contents

List of figures

List of tables

Chapter 1. Introduction

The Republic of Azerbaijan, located together with Georgia and Armenia in South Caucasus, a gateway between Europe and West Asia, marks its 100th anniversary in 2018. The country, roughly the same size as Austria, is a secular and presidential republic. It is a member of the United Nations (UN), the Organization of Security and Cooperation in Europe (OSCE), the Council of Europe (CoE), the Commonwealth of Independent States (CIS), etc., and closely cooperates with North Atlantic Treaty Organization (NATO) and the European Union (EU) [1]. Despite a complicated neighborhood, it is in good relations with clerical Iran, nuclear Russia, NATO member Turkey, and Georgia, which pursues NATO membership. However, Azerbaijan has conflicted with Armenia for more than 25 years. Armenian aggression resulted in the illegal occupation of 20% of the whole territory of Azerbaijan [2]. Despite the political chaos, economic paralysis, and social burden caused by the collapse of the Soviet Union in the early-1990s, as well as the charges of ongoing conflict, the Azerbaijani economy has experienced significant transformation and development. Over the past ten years, the economy of Azerbaijan has grown by 300%, and poverty and unemployment rates stand at 5% [3]. Earlier stages of the rapid economic development of Azerbaijan were mainly due to the exploitation of hydrocarbon resources. However, as of today, Azerbaijan has managed to diversify its economy, making the non-oil sector count for almost 70% of Gross Domestic Product (GDP) [4]. What is more, the Global Competitiveness Report 2016–2017 rated Azerbaijan as the most competitive economy among CIS countries and 38th in the world [5] [6].

Due to the developments described above and developments in building up information society, there is a great need for special measures to ensure cyber security in all critical areas of Azerbaijan, to mitigate the risks of electronic intelligence, electronic countervailing and cyber attacks. The country is rapidly entering the newest projects, and the strategic importance of these projects will inevitably bring the need to ensure the highest level the provision of cyber security.

National Strategy, Laws and Recommendations, the cooperation, etc. are important factors in increasing the country's cyber power. In the developing cyber world, the need for specialized human resources is rising day by day to defend the cyber environment of the country. In addition to administrative reform for cyber security, it is also essential to raise human potential, increase cyber resources of organizations, and implement new co-operatives. From this point of view, the development of national Cyber Security Capacity Building (CSCB) plays an important role in the country. CSCB includes itself, active developing of cyber security potential, human resource capabilities, well-structured cyber security policies and recommendations for organizations and so on.

This thesis evaluates the current state of cyber security in various aspects of Azerbaijan and has been put forward to promote the solution and further improvement of existing problems. The thesis consists of five Chapters. Chapter 1 gives a general overview of Azerbaijan and cyber security threats and risks. Chapter 2 covers research methodology and literature review. In Chapter 3 existing situation in CSCB in Azerbaijan was discussed and analyzed. The following 5 factors were considered while examining CSCB in Azerbaijan:

- Cybersecurity Policy and Strategy
- Cyber Culture and Society
- Cybersecurity Education, Training and Skills
- Legal and Regulatory Frameworks
- Standards, Organizations, and Technologies

The results and analyses of the survey are discussed in the 4th Chapter. The primary purpose of the questionnaire was to get information about experiences and the current situation in capacity-building in Azerbaijan from cyber security and Information Communication Technologies (ICT) experts. The questions given by the author were about stability, legislation, resources, awareness and education, public-private cooperation, human resources, education and training programs, and finally cyber security environment.

In the 5th Chapter, the author proposes an action plan for solving existing problems and gives recommendations for improving CSCB in Azerbaijan. Finally, the conclusion chapter reviews the thesis and summarizes key points of the work.

The thesis has been written in close coordination with CERT Azerbaijan.

Chapter 2. Methodology and Literature Review

This thesis is devoted to the solving CSCB challenges in Azerbaijan based on international experience and local situation. To achieve the goal, the author carried out a literature review of academic literature, guiding documents about cyber security in Azerbaijan, explored different models about international capacity-building models and recommendations. Moreover, to understand existing situation and challenges in CSCB and to propose solutions for solving these problems, various cyber security documentation, national cyber security strategies, policies, and legislation were studied by the author. A survey among cyber security experts and IT professionals was carried out to gain an overview of perceptions of the cyber security environment and to examine the challenges in CSCB in Azerbaijan.

Literature review

"National Strategy on the development of the information society 2014-2020 of the Republic of Azerbaijan" [7] is one of the primary documents from which the cyber security goals of the country were derived. The primary objectives of this direction are ensuring the security of the information space of country, increasing confidence in the use of ICT, the development of normative legislative base which regulates this area and implementation of awareness. To get detailed results of the existing situation, all courses provided in IT field were analyzed and reviewed through the websites of the universities.

The author has defined 5 main dimensions in CSCB to make clear the existing situation and give solutions for existing challenges. In order to come to these dimensions, various CSCB experiences were analyzed. The Global Cyber Security Capacity Centre (GCSCC) is an international center working in research and development in an effective capacity building in cyber security. Moreover, the organization is promoting expansion in quality, effectiveness, scale, and influence of CSCB across the world [8]. GCSCC in partnership with the Global Forum on Cyber Expertise (GFCE), developing projects and solutions for various states and international organizations which aims to enhance CSCB worldwide [8]. The organization deployed Cybersecurity Capacity Maturity Model for Nations (CMM), and it was successfully deployed in more than 50 countries across Africa, Asia, Europe, and Oceania since 2015 [8]. But the existing situation in every state differs, and this model is implemented based on the state’s cyber security capacities. The success and effectiveness of this model made author go through these 5 dimensions and analyze the current situation and propose solutions.

To propose the solution to the CSCB in Azerbaijan, the author used important sources, such as “Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities” by Lilly Pijnenburg Muller [9], “Action Plan 2010-2015 for Canada’s Cyber Security Strategy” by Government of Canada [10], “CYBER SECURITY STRATEGY ACTION PLAN” by Australian government [11].

Survey of IT professionals in Azerbaijan

Online questionnaire, Google forms were used to conduct the survey. For data collection, the author prepared a questionnaire survey using google questionnaire and sent it to the IT and IT security professionals in Azerbaijan. A web-based questionnaire was chosen as it enables time-saving compared to distributing the survey in printed form. The author followed Delphi method which was formulated to get the most reliable opinion agreement of a group of experts by engaging them in a series of questionnaires in-depth analyses with controlled opinion feedback. The Delphi technique was founded by Dalkey and Helmer in 1963 at the Rand Corporation [12]. The method is developed as a team communication process, and it aims to achieve an approach of judgment on a specific issue. The technique is useful in allowing some individuals, to resolve a complex problem [13].

The survey was conducted from March 15, 2018, till April 15, 2018, in English and received 60 responses. The full original questionnaire is in English and can be found in Appendix 1.

Chapter 3. Cyber Security capacity building by factors in Azerbaijan

3.1. Cyber Security volumes and capacity dimensions from the world perspective

The widespread use of computer systems and the penetration of all aspects of our lives has increased our business productivity and facilitated our lives as well as expanding the areas of activity of malicious people and criminal organizations. Malicious people can infiltrate our computer systems, which can cause substantial financial losses for both individuals and corporations. The cyber attacks carried out by some states in recent years in the name of long-term monitoring, manipulation and destruction of political and strategic information pose a significant threat to national security. The human capacity grown in the field of cyber security has become an essential requirement for institutions and commercial companies as well as states today. Nowadays, in numerous progress of cyber security volume, there are severe problems in raising qualified human resource capacity in this area as well.

One of the main points in cyber security is capacity building. New cyber threats, tools, and methods are emerging depending on technological developments. New policies, laws, standards, products, solutions may be needed in the new situation. In this respect, the capacity of policymakers, lawyers (judges, prosecutors, lawyers), software, hardware and application developers have to be developed, and new possible security problems and solutions should be designed. Furthermore, as the nature of cyber crime has changed with technological developments, the technical and administrative capacities of judges and prosecutors investigating these crimes and the law enforcement collecting evidence must be developed to be able to combat new crimes and criminals effectively. For this purpose, various programs are being implemented to increase the capacity of cyber security in multiple countries. Nowadays, UK has a vast experience in cyber security capacity building programs in foreign countries. Regarding the Cybersecurity Capacity Maturity Model for Nations [14] developed by the GCSCC [8], experts defined 5 factors which were explained as, “To facilitate a comprehensive understanding of effective and efficient national cyber security capacity and to enable policymakers to define priorities for capacity building and investments [8].” The author has chosen this model as a basis, because the model has successful effects in a world wide as a CSCB solution and includes itself all areas cyber security for building strong cyber security platform. The five dimensions defined are the following:

- Dimension 1: Cybersecurity Policy and Strategy
- Dimension 2: Cyber Culture and Society
- Dimension 3: Cybersecurity Education, Training and Skills
- Dimension 4: Legal and Regulatory Frameworks
- Dimension 5: Standards, Organizations, and Technologies

3.1.1. Dimension 1: Cyber security policy and strategy

At the point where information technologies come; it is evident that this phenomenon, which is expressed as "Cyber Space," has emerged beyond physical boundaries and rules, has gone beyond being a rumor and has become an undeniable reality that has been stripped away from the virtual world. Now, in the world, nearly all kinds of services and activities take place in cyber space. Cyber space also brings along these opportunities as well as risks. Cyber attack, cyber crime, cyber terrorism and finally cyber warfare; all increasingly affect every part and level of cyber space. And it makes compulsory to provide security in the cyber space. This necessity, expressed as cyber security, cannot be achieved in a dispersed and unacknowledged and uncoordinated way, away from facts and examples of contemporary practice. Cyber security is critical in many fields such as administrative, technical, sociological, historical, legal, political, military and academic. Handling cyber security issues in the right way and direction is possible only by determining the principles and strategies.

Considering that any initiative for which the principles and strategies are not clear is considered to face huge risks; the formation and implementation of the Cyber Security Strategy in environment shaped like the future of Cyber Space, is crucial to successfully implement the empowerment and cooperation of all stakeholders: citizens, governments, public institutions and organizations, private sector, universities and non-governmental organizations.

In this thesis, Cybersecurity policy and strategy are looked at the level of national and organizational legislation. It covers national strategies and policies.

3.1.2. Dimension 2: Cyber culture and society

The concept of cyber culture originates at the junction of two worlds - physical and virtual [15], as computer networks and technologies are increasingly being introduced into our daily lives, entertainment, communications, and business. Given the complexity of giving an unambiguous definition of the boundaries of cyber culture, the use of this term to describe various phenomena in society is very vague and contradictory. Manifestations of cyber culture are based on interpersonal interaction in which computer networks act as mediators [15]. They can be expressed as actions, aspirations, games, places, and metaphors and include a diverse range of applications. Some are supported by specialized software, while others use standard web protocols. As examples of manifestations of cyber culture in modern life, we can specify the following: blogs; social networks; network games; online chats; forums; electronic bulletin boards; e-commerce; peer-to-peer network; virtual worlds; and so on.

Cyber culture and society are broad areas and differs depending on the country. Cyber society terminology is considered to the information society [16]. In this thesis, the author described Azerbaijan’s existing cooperation with foreign countries, state-level actions in order to improve citizens’ online security, provide online services and facilitate their internet usage.

3.1.3. Dimension 3: Cyber security education, training and skills

It is necessary to prepare national and international developed programs in order to develop qualified human resources required in the field of cyber security. The establishment of graduate and postgraduate level programs in cyber security, research institutes and test centers and certification programs should be encouraged by the state. Additionally, cyber security training courses have to be organized and provided from low to high-level knowledge and skills to the people. The purpose of these educational programs is to raise awareness level, cyber security knowledge, skills of citizens and information technology specialists. Moreover, to fulfill individual and institutional obligations, it is necessary to organize activities that will raise the level of knowledge and awareness for cyber security stakeholders who are citizens, the business, and trade and government organization. Educational programs can be long term which should be taught from the first school and short-term, like graduate programs and training courses.

In this thesis, Cybersecurity education, training, and skills are investigated in a university and personal training courses level. The author analyzed existing IT and Cyber Security related courses in universities and training centers.

3.1.4. Dimension 4: Legal and regulatory frameworks

The scope of cyber space is growing at a rapid pace, and with it, the level and complexity of threats to the states and threats to their information technology systems and infrastructure are increasing as well. The use of cyber elements to achieve political, economic, military objectives or to obtain a geopolitical advantage is part of our present reality. The emergence of an increasing number of players in cyber space expands the range of used attack methods and the number of systems that can become their potential targets. On the other hand, government information and communication systems, military and commercial projects are becoming more vulnerable to cyber attacks and cyber espionage. From this perspective, it becomes crucial to managing cyber space of country from the state level. The law of cyber security establishes the legal and organizational framework for ensuring cyber security of the state, directions, and principles of state policy in the field of cyber security. And also the powers of state bodies, enterprises, institutions, organizations, individuals and citizens in this sphere and the basic principles of coordination of their activities. According to the cyber security law, it is expected to increase the function of the governmental regulators, duty separation of security organizations. Furthermore, define the procedures and principles regarding effective supervision, duty to keep secrets, tasks of response teams to cyber incidents, corporation of public-private organizations with state services, various sanctions which will be applied to companies that do not take control security vulnerabilities.

Author’s approach to this dimension was analyzing existing legal and regulatory frameworks in cyber security in Azerbaijan’s legislative framework. Laws, doctrines, improvements existing legislation were considered.

3.1.5. Dimension 5: Standards, organizations, and technologies

Sustainable cyber security is only possible with the generation of new technologies. Though it is possible to supply generation and innovative new technologies from abroad by purchasing; this approach is not acceptable for advanced and complete security. It is also sometimes not possible to know or determine that cyber security technologies supplied from abroad do not contain malware such as backdoor and Trojan horses.

That is why close monitoring of new generation, innovative and intelligent technologies; developing of national and original approaches, solutions and techniques are important. The projects which are the national operating system that can support the cyber security field, the national Internet browser, and the national search engine, development of national software and hardware are important regarding prevention of external dependence and sustainable development. Within the scope of cyber security, malware prevention, virus prevention, firewall, intrusion detection and prevention systems should be developed with national resources, the private sector should be encouraged to produce national technology, and these products should be encouraged to be used in public and private sector. Within the context of information technology and cyber security, it is necessary to establish national testing and national certification centers and national protection profiles, especially in the context of product safety. The following reasons make compulsory to develop cyber security standards, organizations technologies in national level.

Existing organizations, international cooperation, applied standards, local security agencies are looked in Azerbaijan according to the 5th dimension.

3.2. Cyber security capacity building situation in Azerbaijan by five factors

3.2.1. Cybersecurity policy and strategy

Over the past decade, national governments have been developing strategies to address emerging security issues associated with the rapidly expanding use of ICT. These cyber security issues have evolved into significant national-level problems that require government consideration, including the protection of assets, systems, and networks vital to the operation and stability of a nation, and the livelihood of its people. Threats against these critical assets target corporations and citizens and include cyber crime such as identity theft and fraud, politically motivated -hacktivism, and sophisticated economic and military espionage [17].

In many countries, national policy has become a priority supported by stronger leadership. A single determination of information security cannot be obtained from these strategies. Nevertheless, all new plans are becoming integrated and comprehensive. They holistically approach cyber security, encompassing economic, social, educational, legal, law-enforcement, technical, diplomatic, military and intelligence-related aspects [18]. As in many countries, developing national cyber security policy is essential for Azerbaijan as well.

Apart from legal documents that are related to cyber security, some policies concern cyber security. It is important to mention that there is no separate strategy on cyber security or cooperation with the private sector on the issue, but there are some provisions of various policies that are related to developing cyber security capabilities. These strategies are "National Strategy on the development of information society for 2014-2020" [19] and "2016-2020 State Program on the implementation of National Strategy for the development of information society" [20], "Azerbaijan 2020: Concept of Development” [21], and "Strategic Road Map for the development of communication and information technologies.” [22]

“The National Strategy for Development of Information Society in Azerbaijan during 2014-2020” [19] considers all experiences and recommendations which have been made by ITU and the EU. The main aim of the Strategy is "to build an information society and efficient use of its capabilities by citizens, community and the state for the sustainable socio-economic, cultural and economic development of the country, including the development of ICT" [23]. The Ministry of Communication has been assigned the coordinating role for implementation. The article [24], which was published in CyberCrime@EAP journal, mentioned that the Strategy encompasses most aspects of cyber security. Achieving information security is among the top priorities. The goals of this priority are to develop security of digital space, to increase trust in the utilization of the ICT, to upgrade the legal framework, and to raise awareness. Objectives for reaching these goals include creating state policy on information security, decreasing dependence on foreign countries in terms of information security, protecting ‘e-government’ networks, announcing cyber threats on a nationwide level, developing technical expertise in cyber security, strengthening ‘safe Internet' for children, raising awareness in society and among companies, and promoting information security culture. Two primary objectives applicable to this research are to develop information security of Critical Infrastructure and coordinate cyber security activities of state and non-state bodies [19]. The strategy is implemented in two stages, each stage being accompanied by the state programs [23]. The State Program for 2016-2020 [20] consists of concrete steps on seven priorities for the implementation of National Strategy. According to the action plan for information security, the Ministry of Transport, Communications and High Technologies (MinCom), State Security Service (SSS), State Agency and Ministry of Defense (MoD) are responsible for updating normative legal acts on cyber security, monitoring the security of information networks and resources, securing ‘e-government,’ establishing formal relations and cooperating on cyber security with foreign counterparts. The goals of the Program include ensuring digital security space of the country and increasing cyber security capabilities of state and non-state bodies as well as private individuals [25]. The “Azerbaijan 2020: Look into the Future” [21] Concept of Development is the strategic plan for overall development of the country in all sectors. The concept is a result of collaboration between state bodies, education organizations, high-profile experts, international organizations, civil society organizations, and citizens. Development of ICT and the transition to an information society are among the top priorities. One of the primary objectives is information security. The concept covers prevention of cyber attack, the safety of information processes, security of information resources and networks of state bodies, and nation-wide cyber security preparedness [26]. According to the Strategic Road Map [22]for the development of communication and information technologies and SWOT analysis of the ICT sector in the country showed that increasing challenges to network and information security are among the leading threats. One of the strategic goals is to enhance national cyber security preparedness and awareness [22].

3.2.2. Cyber culture and society

Cyber Culture and Society terms are associated with information society and culture in Azerbaijan. The information society is such a society where most members of the community are engaged in the production, storage, processing, and use of information [27]. From past years, Azerbaijan is actively participating in the development of information society and increasing the capacity of information recourses. From this perspective, we can mention federal decrees, orders, decision and rules corresponding to the information society. The table below includes some legislative acts which emphasize the developing information society and making it versatile.

Table 1. Legislation on cyber culture and society [28].

Name	**Date**
Law of the Republic of Azerbaijan on Electronic Signature and Electronic Documentation	2004
Law of the Republic of Azerbaijan on Access to Information	2005
Information, Informatization, and Protection of Information	2017
Decree of the President of the Republic of Azerbaijan on measures for e-government development and transition to digital government	2018
The decision of the Cabinet of Ministers of the Republic of Azerbaijan on "Approval of Requirements for Establishment and Management of Internet Information Resources by State Agencies" (No. 189).	2012

As a result of increased demand for internet services and technical capability in the country, the entire international internet channels increased by 80 Gb/s to 330 Gb/s in 2014 [29]. Thanks to the capacity of foreign internet channels in recent years, Internet traffic from Georgia, Iran, Iraq and Central Asia is transmitted through Azerbaijan [29].

With the introduction of the latest technologies in every settlement in the country, a "national broadband internet development" project has been developed, covering high-quality Internet access and modern communication services. The implementation of a component of the project has already started. As a result, over the past five years, the internet market has grown 3.2 times and now amounts to $ 145.1 million [29]. 75 out of every 100 people in Azerbaijan are Internet users, and 65 are broadband Internet users [29].

One of the valuable and useful projects of Azerbaijan government is the "e-government." The work, which was carried out in the field of application of "electron government", has gained wider coverage with the adoption of the "State Program for Development of Communication and Information Technologies in the Republic of Azerbaijan for 2005-2008" (Electronic Azerbaijan) and 2010-2012 the second "Electronic Azerbaijan" State Program and "Action Program on Formation of «Electron Government» in the Republic of Azerbaijan" [30]. In addition to these programs, "e-government" project is being implemented within the framework of up to 20 state-run economic and social programs [30]. To provide the exchange of information systems of state bodies and use of governmental electronic services by citizens' www.e-gov.az "electronic government" portal has been created. Currently, the e-government portal has been integrated into 39 information systems of state agencies and has provided over 200 e-services through this portal [30]. The "e-government" gateway enables the government to efficiently utilize existing information systems, secure communication between them, provide inquiries, respond to them, and with centralized document management prevent getting additional paper documents from the citizens.

Moreover, Azerbaijan has active relations with foreign countries in sharing and implementing international experience. Azerbaijan is actively cooperating with Estonia in digital development and information technology from 2009 [31]. One of the great examples is the deployment of "Asan Imza" in Azerbaijan in cooperation with Estonia [32]. The mobile identity service and the digital signature of "Asan İmza," provides ubiquitous and secure access to the public and private electronic services. Digital mobile signature is equated to a national identity at the legislative level [33]. Being an indispensable tool in all spheres of the economy, "Asan İmza," based on the public key infrastructure (PKI), allows us to identify a person, put a digital signature equal to the citizen's name by the law of the Republic of Azerbaijan [33].

Currently, more than 500 public and private electronic services in Azerbaijan are using "Asan Imza" in their systems. Along with this, the digital signature has been integrated into the call-centers of various governmental and private structures, today filing electronic tax returns, declaring goods and transport services in the customs service, registration of notices of employment contracts, online registration of applicants is based on "Asan Imza." [33]

Approved laws and decrees give impetus to the development of information society in Azerbaijan. However, there are still many shortcomings, such as the lack of national content, the lack of written and virtual information on information technology in Azerbaijani, the lack of national games and forums and so on.

3.2.3 Cyber security education, training and skills

Education and training in Information Technologies.

In recent years, many universities and other educational institutions have been interested in education in this area because of the development of information technologies in Azerbaijan [34]. From this point of view, individual universities in Azerbaijan have provided space for teaching information technology as bachelor and master degree education program. Examples of such universities are Khazar University, Baku Engineering University, Azerbaijan Technical University, Western Caspian University, ADA University, Azerbaijan University, etc. In addition to the university, there are many private training centers in Azerbaijan. Local IT Consulting and Training Centers such as STEP IT Academy, Softline, and Code Academy are providing courses about various fields of IT. However, software programming and database administration, systems and network engineering are the primary programs taught in universities and education centers. Next paragraph describes the contents of the IT-related educations programs in Azerbaijan. The information provided is based on interviews with educational institutions and civil servants, as well as analyzing web sites of universities in Azerbaijan.

IT related programs and contents in Azerbaijan universities.

Higher educational institutions are divided into four groups in the Republic of Azerbaijan [35]:

- ◦ Higher education institutions under the Ministry of Education (20 Universities)
- ◦ Higher education institutions subordinated to other ministries and committees (12)
- ◦ Private Higher Education Institutions (11)

◦ Special-purpose higher education institutions (7)

The groups mentioned above respectively consist of 20, 12, 11 and 7 universities and more top education schools. All these educational universities offer both bachelor, masters and doctorate degrees.

In addition, the universities specializing in technical education, such as Khazar University, Baku Engineering University, Azerbaijan Technical University, and other universities are providing information technology education, however, universities such as Western Caspian University, ADA University, Azerbaijan University and others, which mostly focus on administration and management, are also teaching information technology.

More specifically, the bachelor's and master's degrees offered by each university in the field of information technology are listed in the following table:

Table 2. Higher Level IT education in Azerbaijan.

University	Bachelor	Masters	Link

Khazar University	Computer Science;
	Computer Engineering;
		Computer Science;
		Computer Engineering;
			http://www.khazar.org/en/menus/392/bakalavr_proqrami
			http://www.khazar.org/en/menus/181/magistr_ve_felsefe_doktoru_proqramlari

Azerbaijan University	Computer Engineering;	Computer Sciences (Mathematical and information support of economic activity);	http://www.au.edu.az/en/menu/102/komputer-muhendisliyi http://www.au.edu.az/en/menu/39/
Baku Engineering University	Computer Engineering;	Computer Engineering;	http://beu.edu.az/en/pages/Bachelors-903317.html http://beu.edu.az/az/pages/Magistaturaya-q%C9%99bul-903116.html

Western Caspi University	Information Technologies;
	Computer Science;
	Computer Engineering;
		Computer Science;	http://wcu.edu.az/en/undergraduate
			http://wcu.edu.az/en/masterdegree

Azerbaijan Technical University	Information technology and systems engineering;
	Process Automation Engineering;
	Computer Engineering;
	Computer Science;
		Systems and networks;
		The technology of data protection and organization;
			https://aztu.edu.az/azp/academic/bachelor.do
			https://aztu.edu.az/azp/academic/master.do

ADA University	Information Technologies Computer Science Computer Engineering	N/A	http://www.ada.edu.az/Pages/school_of_information_technologies.aspx http://www.ada.edu.az/en-US/Pages/apply_graduate.aspx
Azerbaijan State University Of Economics	Engineering of IT and Systems;	Information technologies of the world economy;	http://unec.edu.az/en/education/training-programs/

The courses in these faculties are approximate consists of the same content and direction. Information technology and computer engineering faculties mainly covered by the following directions:

- Computer software and hardware
- The basics of programming
- The programming and operating system

- Digital systems
- Computer networks
- Web programming and design
- Computer schematics appliances and microprocessor systems
- Object-oriented programming
- Computer graphics
- Database management systems
- Nanotechnologies
- Automation computing experience
- Intelligent systems

As we can see from this outline, higher education institutions in Azerbaijan do not offer any bachelor or master degree programs related to the cyber security and cyber security is not included in the existing programs. This is one of the first problems in training new cyber security professionals in this country. Many private education companies are providing various lectures and courses in Azerbaijan. These include both local and foreign courses. The best of them and the world-famous ones are the IT Step Academy and Softline. IT Step Academy is also an authorized education center of Microsoft, Cisco, Autodesk, in addition to operating in 16 countries worldwide [36]. Students of the Academy receive international certificates free of charge while finishing the course. However, among the courses offered by the academy the "Network and cyber security" course is closer to the cyber security. Nevertheless, the knowledge and skills taught by the course are mostly focused on operating systems and networks. This situation is more common in various courses in Azerbaijan. The contents of the courses are consisting of the following areas [37]:

- Computer software and hardware
- CCNA and CCNP

- Network Security technologies
- Administration Windows Server and GNU/Linux operating systems
- Oracle and Microsoft SQL Server Administration
- Various programming languages

As well as the “Softline” which is operating in 30 countries of the world and the local private educational center "Code Academy" does not offer cyber security courses [38]. "Softline” is famous for the system and network engineering sphere, and Code Academy is specialized in programming.

3.2.4. Legal and regulatory frameworks

As cyber crimes, particularly cyber terrorism is getting more dangerous, there is a high demand to improve the activity of the responsible state bodies in this field to prevent cyber threats in Azerbaijan. The existence of necessary technical opportunities, as well as knowledge and skills, are essential for practical struggle against illegal activities in the relevant sphere. During the recent years, adequate measures have been taken to improve opportunities for prevention of cyber threats.

Currently, as the number and complexity of cyber threats, cyber crime tools, and attack instruments have rapidly increased, the number of cyber crime cases are raising significantly around the world.

In 2009, after joining of Azerbaijan to Convention “On Cybercrime” Council of Europe [39] and ratification and enactment by the Parliament, there were implemented significant reforms on combating against cyber crime. In 2012 the legislative framework on fighting against cyber offense was improved, and it was adapted to the requirements of the Convention. Some articles were intended in the Criminal Code of Azerbaijan [40] related to committed crimes and acts. In accordance with the needs of the Convention, Ministry of National Security of the Republic of Azerbaijan was appointed as coordinating body which is available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. According to the Decree of the President of the Republic of Azerbaijan [41] - Special Communication and Information Security State Agency of Special State Protection Service of the Republic of Azerbaijan and Cyber Security Service under the Ministry of Transport, Communications, and High Technologies were established in 2012.

Some measures are being implemented for awareness and educating of the population in the field of information security. That is great importance for any country including Azerbaijan, in order to secure store and transmit data in public and private sector. The number and level of cyber security experts in Azerbaijan are not enough to meet the cyber security challenges. Improving the capacity of specialists is important for the country to increase the level of cyber security. Table 1 provides an overview of legislation on cyber security in Azerbaijan's cyber security architecture.

Table 3. Law on cyber security.

Name	**Related provisions**	**Date**	**Reference:**
National Security Concept	4.3.11 Information security policy	2007	http://www.e-qanun.az/framework/13373
Convention on Cybercrime	All	2009	http://www.e-qanun.az/framework/18619
Military Doctrine	50.1 Main responsibilities: Information infrastructure 61. Development priorities: Information infrastructure	2010	http://www.e-qanun.az/framework/19722
Improvement of activities in the field of information security	All	2012	http://www.e-qanun.az/framework/24353
Law on National Security	20. Ensuring national information security	2012	http://www.e-qanun.az/framework/5455
Criminal Code	Chapter 30. Cyber crimes	2012	http://www.e-qanun.az/code/11

Statute and structure of Special Communication and Information Security State Agency under the SSPS	N/A	2012	http://e-qanun.az/framework/24735
Ensuring activities of Cyber Security Service	All	2013	http://www.e-qanun.az/framework/25375
Information, Informatization, and Protection of Information	All	2017	http://www.e-qanun.az/framework/3525

3.2.5. Standards, organizations, and technologies

Apart from developing national cyber security capabilities, Azerbaijan also works with other countries bilaterally, participates in intergovernmental organizations, and cooperates with global firms which specialize in cyber security. Indeed, the objective of expansion of bilateral and multilateral cooperation in the field of cyber security is mentioned explicitly in the National Strategy on the Development of the Information Society 2014-2020 [7]. It should be noted that Azerbaijan has officially recognized international cyber security standards through the State Committee for Standardization, Metrology, and Patents [42]. Azerbaijan is a member of the ITU-IMPACT initiative of the International Telecommunications Union, FIRST, Trusted Introducer, Anti-Phishing Working Group (APWG), etc. [43]. Azerbaijan also cooperates with the US-based Symantec, the most significant anti-virus software production company [44]. Bilaterally, Azerbaijan closely works with Japan, Russia, Ukraine, the Republic of Latvia and the Republic of Slovakia on addressing computer-oriented criminal activities [45]. Azerbaijan is also one of the most active partners of NATO on a range of issues [46]. These include cyber security via the NATO Cooperative Cyber Defense Centre of Excellence. It should also be noted that Azerbaijan is a staunch supporter of international cyber laws [47]. In 2008, Azerbaijan joined the Convention on Cybercrime [44], which covers "Internet crimes including misuse of the computer networks, infringements of copyright, computer-related fraud, child pornography and violations of network security."

Indeed, Azerbaijan has introduced the "Internet Access and Infrastructure Development for Research, Education and Civil Society Development Purposes" project [48], and is working together with the ITU on the development of a global convention on information security.

To research international experience and implement it in Azerbaijan, cyber security organizations became full-fledged members of international unions such as "OIC CERT," "Trusted Introducer," "APWG" and "FIRST." Additionally, the country started cooperation with computer emergency response teams of more than twenty countries. On the other hand, national cyber security response teams of Azerbaijan started to get security reports from the leading companies and unions, such as Google, Shadowserver, Microsoft, APWG, FIRST, Team Cymru, Open Phish Team and Trusted Introducer.

To understand the full picture of cyber security and cooperation among stakeholders, it is essential to look at how small and medium-sized enterprises (SMEs) are involved in the overall cyber security of the country. SME-s account for 70% of Azerbaijan economy [[49]]. As mentioned earlier, their cyber-security capabilities are only limited to their IT departments, and the government treats cooperation with them on cyber protection the same as it would treat participation in any other sector which does not carry the equal importance for the state and society overall. The CERT Azerbaijan has been officially recognized as the national program for PPP for sharing cyber-security assets with non-state actors [50].

In general, the CERT Azerbaijan is a coordination point and cooperates with all companies. For example, if any business is faced with a cyber threat or accident, either company notifies the Service, or the Service itself detects the cyber incident on the network or system of a given company during regular monitoring and notifies that company. After being informed about a cyber-incident, the Service works with organizations on prevention or mitigation, depending on the situation. Its activities regarding partnership with businesses include, but are not limited to, testing security of information systems by invitation of companies, informing companies about infringement to their systems, as well as reporting about potential threats, assisting companies in developing their cyber security capabilities and preventing risks, examining cyber incidents, presenting results of investigations to law enforcement organizations, and organizing training sessions to employees upon company request [51].

The Service is considered to be viewed as a bridge between businesses, Internet providers, state law-enforcement agencies and the general public. For maintaining secure digital space of the country, it works with national Internet providers, such as AzTelecom, Delta Telecom, AzerTelecom, etc., and other government bodies such as Special State Protection Service (SSPS), SSS, Ministry of Internal Affairs (MIA), etc. Depending on a situation, it involves any of the entities mentioned above for investigation of infringement [52]. Other tasks of the Center could be summarized as analysis of general cyber safety in the country, coordination of activities regarding cyber security of all companies and relevant state bodies, collection and analysis of information on cyber incidents received by individual users, companies, software manufacturers and similar organizations of foreign countries, awareness-raising on cyber security measures, preparation of bulletins, instructions and recommendations about the acquired information and so on [52]. As it can be seen, cooperation is based on SMEs voluntarily notifying the Center about cyber incidents and on the Center's monitoring responsibilities.

Cyber security organizations and internet service providers built their security infrastructure in the last five years. National cyber security laboratory has been established by Cyber Security Service in 2014 and developed in 2016 by world-known Cisco Company. Although some organizations created security operations centers, Azerbaijan is still in need of national security operations center to monitor and secure the general internet traffic of Azerbaijan, monitor real-time attacks and provide overall security of Azerbaijan. On the other hand, National Cyber Security Service of Azerbaijan includes penetration testing, malware analysis, incident response, attack examinations and other services for private companies, banks, and financial organizations, and also public agencies under the Ministry of Transport, Communications and High Technologies.

3.3 Cyber security capacity building in Azerbaijan – experts view

The following part aims to analyze the existing situation and challenges in CSCB in Azerbaijan. 5 main dimensions, as described above, were taken into account and constructed from stability, legislation, recourses, awareness and education, public-private cooperation, human recourses, education and training programs and finally environment aspects.

3.3.1 Collection of data

For data collection the author prepared a questionnaire survey and sent it to the IT and IT security professionals in Azerbaijan. The author followed Delphi method which was formulated in order to get the most reliable opinion agreement of a group of experts by engaging them to a series of questionnaires in depth analysis with controlled opinion feedback.

Thus, the prepared questionnaire has been sent to approximately 80 experts and 60 of them responded with their relevant feedbacks. Demographic information about participants has been given in the following section.

3.3.2 Demographic data on participants

As it was described before, following the Delphi method the questionnaire has been sent to approximately 80 experts of Azerbaijan to gather their feedback. 50 of these participants are cyber security specialists and information technologies professionals who work in public and private organizations of Azerbaijan. Their profession varies: cyber security experts, cyber security heads, cyber security managers, lawyers in the field of information security and other professionals are from different areas of information technologies. Hence, 16 cyber security experts and 44 other IT professionals participated in this survey.

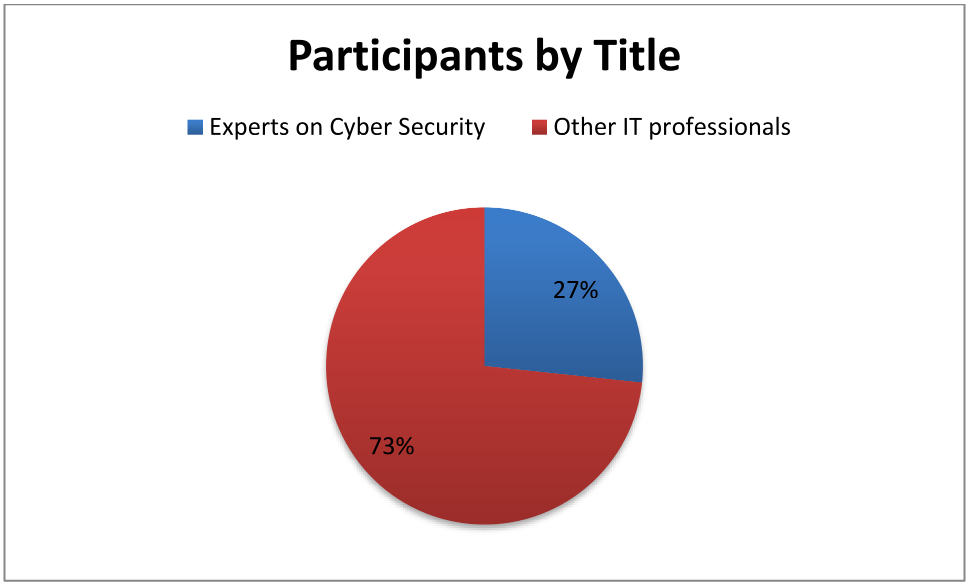

Figure 1. Participants to the survey.

As their experience varies, this was classified into 5 groups based on years of experience in the field: “1-3 years”, “less than 1 year”, “3-5 years” and “more than 5 years”. Based on this groups 6 of participants has less than 1-year experience, 10 experts are from “1-3 years” group, 14 experts have 3-5 years’ experience, and the rest 30 specialists have more than 5 years’ experience.

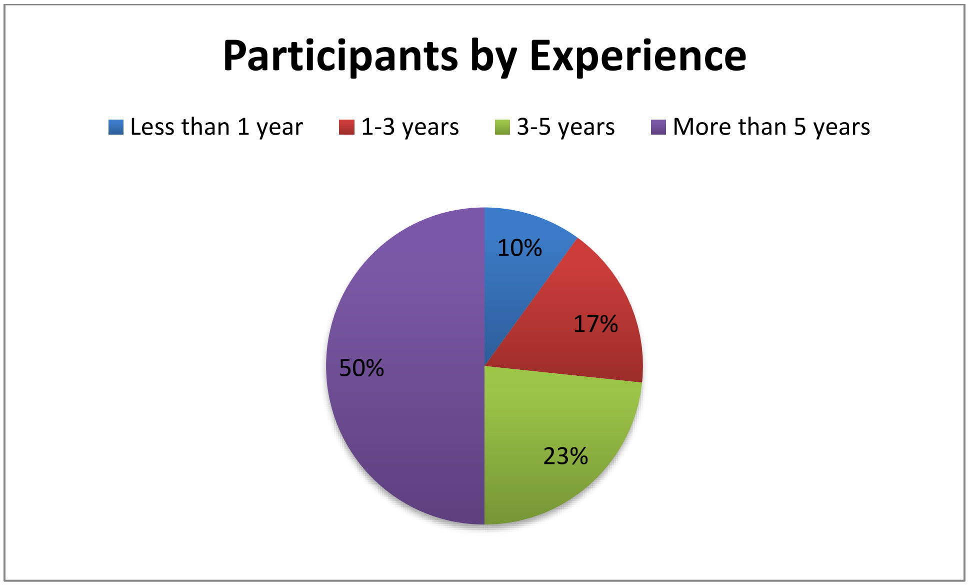

Figure 2. Participants to the survey.

48% (29) of respondents are working in private sector and 52% (31) are professionals from different public organizations which is really useful in terms of research and feedbacks:

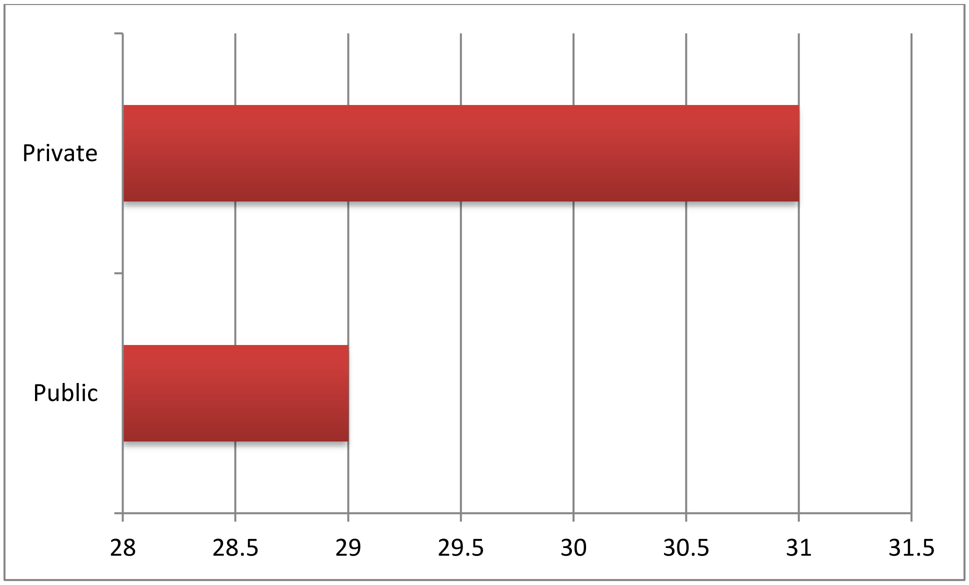

Figure 3. Participants to the survey.

Considering the fact that number of female professionals in the field of information security is sharply differs from number of male specialists, just 6 female experts participated in this research which constitutes just 10% of all respondents. The following figures show detailed information about participants:

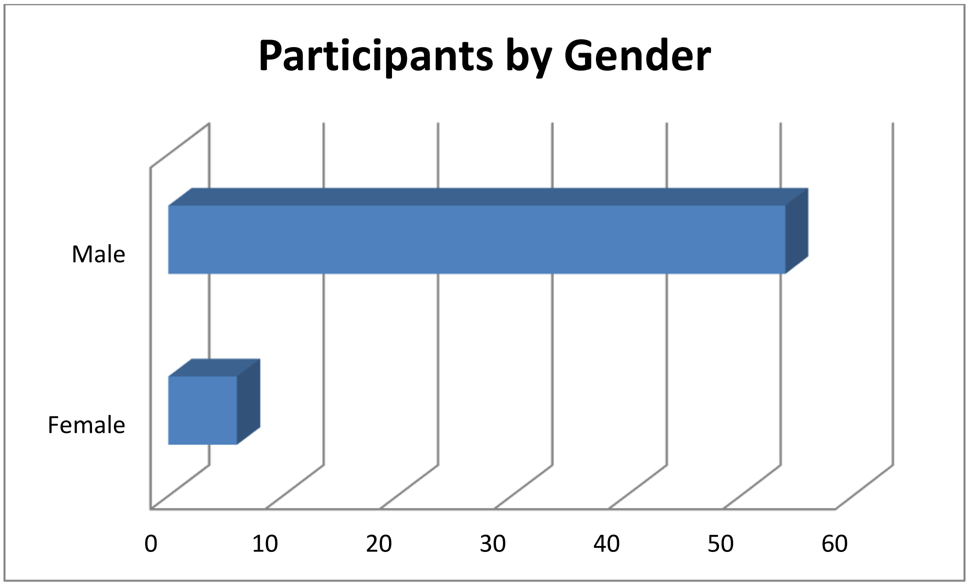

Figure 4. Participants to survey.

3.3.3 Analysis of experts' feedbacks

It is important to note that the author analyzed the data and displayed results based on experts' feedbacks. As mentioned before, data was collected from 60 experts in cyber security and other IT professionals. The survey questionnaire has been developed and sent by email and data was collected anonymously.

The survey contains 10 main parts which describes demographic data on participants and 9 different aspects of capacity building. Brief information on demographics of the participants was given in the previous section. The detailed information on aspects which were considered in the preparation of survey is provided below.

1. Stability. Access to cyberspace is growing faster than the frameworks and organizations that nations use to support it. This growth in access is positively received in the developing countries as it allows more people to connect to cyberspace and the Internet, which in turn is seen as a to boost the economy [53]. It is essential for the country in question to have a clear understanding of its own capabilities and equally of what needs to be strengthened.

IT security and other IT professionals state that the existing capacity in 26.7% of organizations in Azerbaijan is enough to build a cyber security team. However 21.7% of the professionals disagree with this statement. 15% of the responders strongly agree that the organization they work is capable to develop a team for cyber security and just 4.7% of them strongly disagree with this.

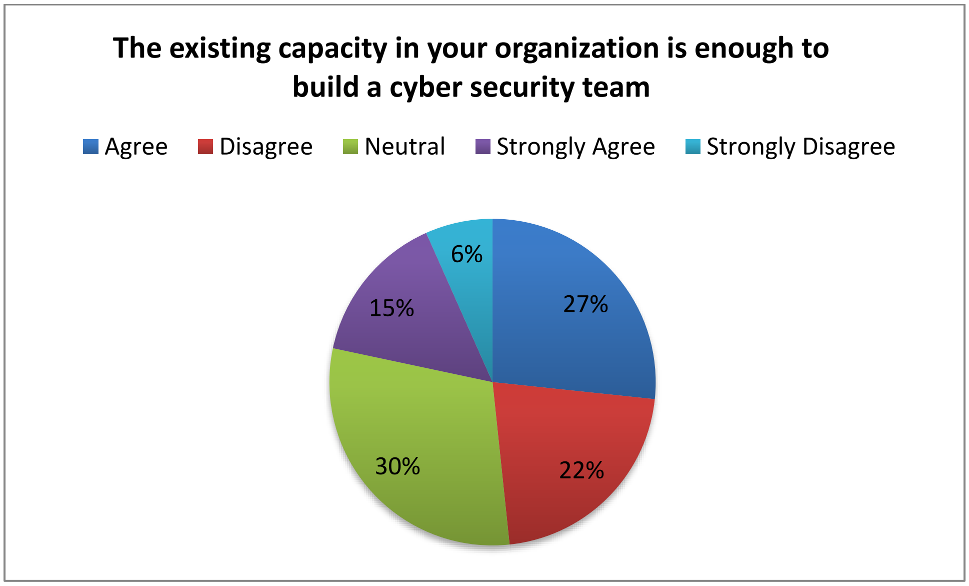

Figure 5. Current capacity in organizations to build a cyber security team.

In 30% of the organizations cyber security knowledge of current professionals is enough to protect the organization. The number of experts who disagree with this statement is slight less; hence it is 16 of 60.

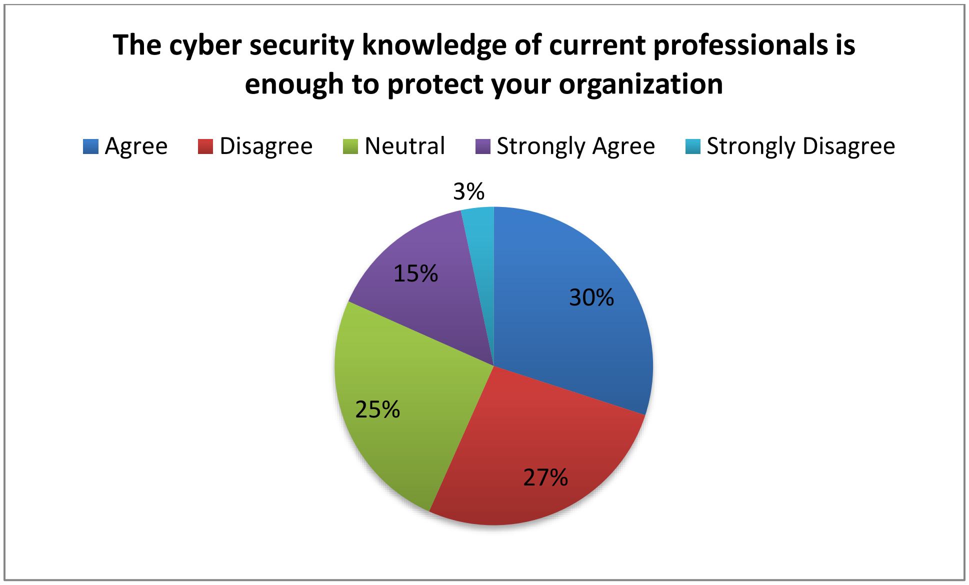

Figure 6. Knowledge of professionals to protect organization.

Statistics show that decision makers or responsible people in 40% of organizations know the needs to improve cyber capacity, besides 26.7% of decision makers strongly agree with this statement. Feedbacks describe that 15% of responsible persons do not know the needs.

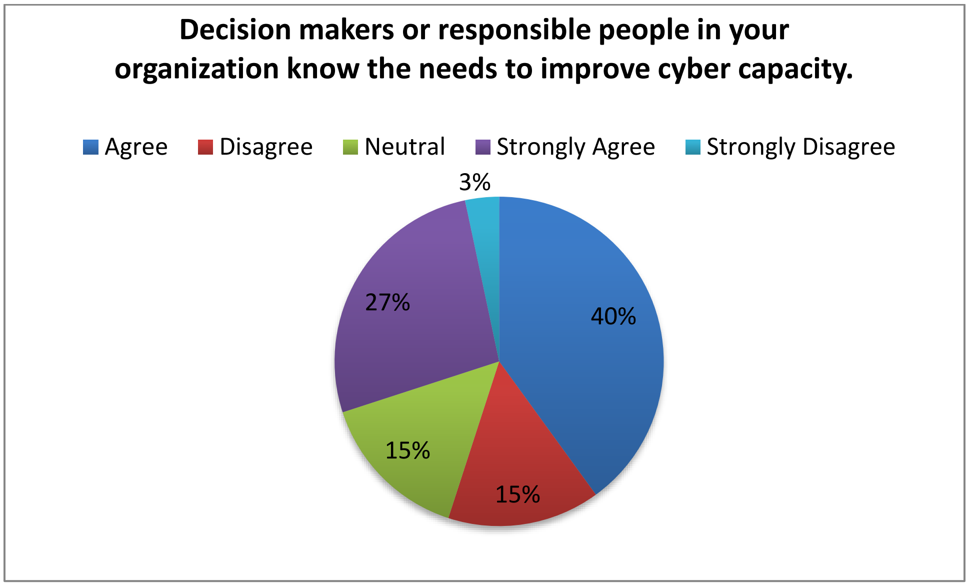

Figure 7. Decision makers know the needs to improve cyber capacity.

2. Legislation. States have the role to take measures in the regulatory or legal field to clarify, improve, and enforce domestic laws related cyber crime. In this context, governments also have the responsibility to promote the interoperability over the legal frameworks developed by other countries.

Basically, the policy argument must be done clearly from everyone in public. This is an area where transparency is produced not only by keeping information from the public (with an intention that it would compromise the company blueprint or notify criminals about loopholes) but also through the generality of issues and legislative proposals so widen and incomplete then, it becomes impossible to understand what powers are granted and the purposes they will be used.

The feedbacks have been provided by experts show that 51.7% of organizations have cyber security policy; however, 28.3% of them do not have any approved cyber security policy. Hence without cyber security policy it is not possible to develop cyber security capacity.

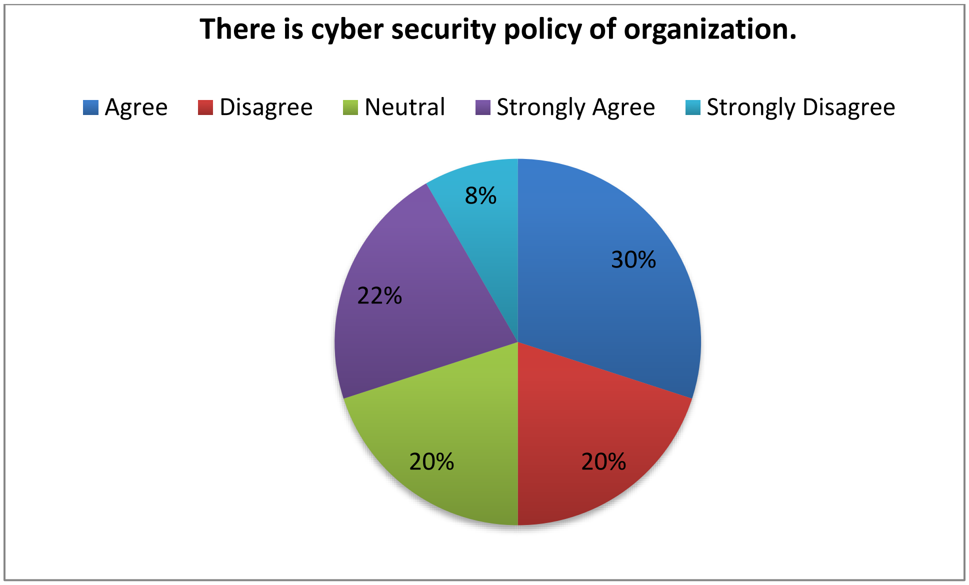

Figure 8. There is cyber security policy of organization.

33.3% of the experts agree that the existing legislative frameworks in their organizations are enough for building cyber security capacity and 28.3% of the responders are sure about this. On the other hand, 28.3% of the experts disagree with this statement.

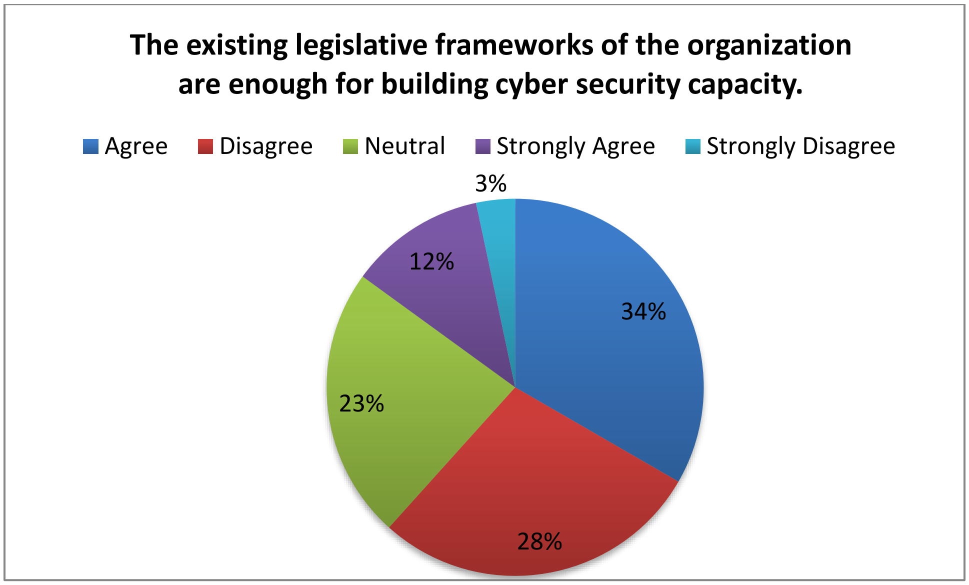

Figure 9. Legislative frameworks.

There is enough number of guidelines for building cyber security capacity in 41.7% of organizations, but there is lack of such guidelines in 16.7% of organizations.

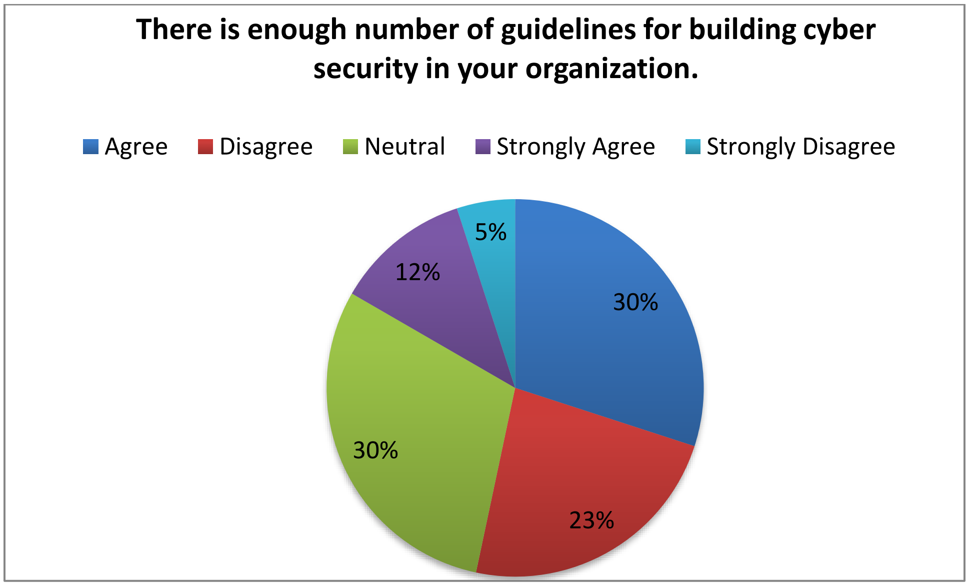

Figure 10. Guidelines.

3. Resources. When weighing investment in cyber security against other business needs, senior management needs to consider the overall level of cyber risk, their agency's exposure to such risks, and the potential whole-of-business cost that could be incurred if a serious cyber incident were to occur on their network. The costs of compromise are almost certainly more expensive than preventative measures.

Many countries lack resources to build what they need to construct and secure capacities in cyberspace. Implementing frameworks and infrastructure is of limited use if the receiving country does not have the capacity to maintain it.

60% of the experts, who responded to the survey for the current research state that the existing financial resources of the organizations are enough to build cyber security capacity building, improve the skills of current professionals and protect the organization.

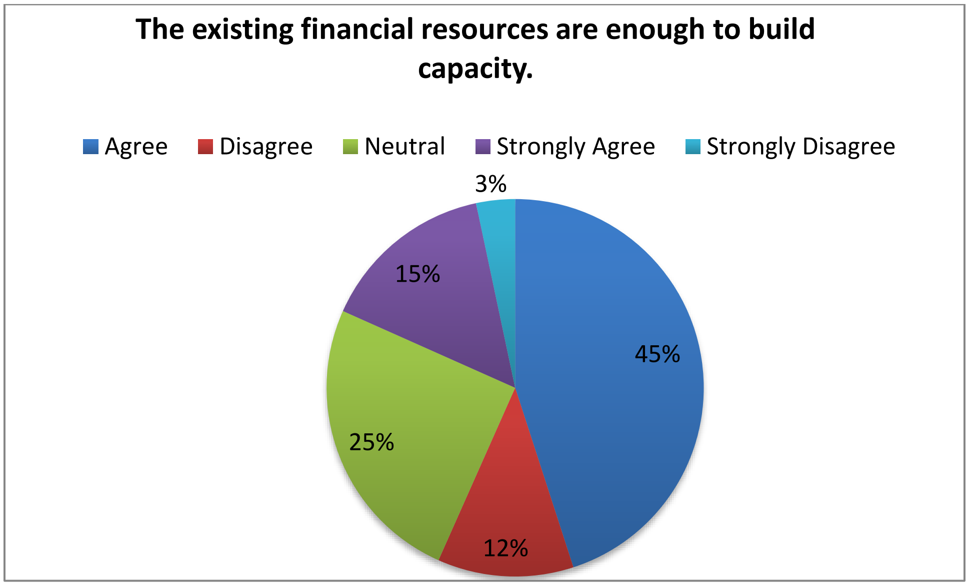

Figure 11. Financial resources.

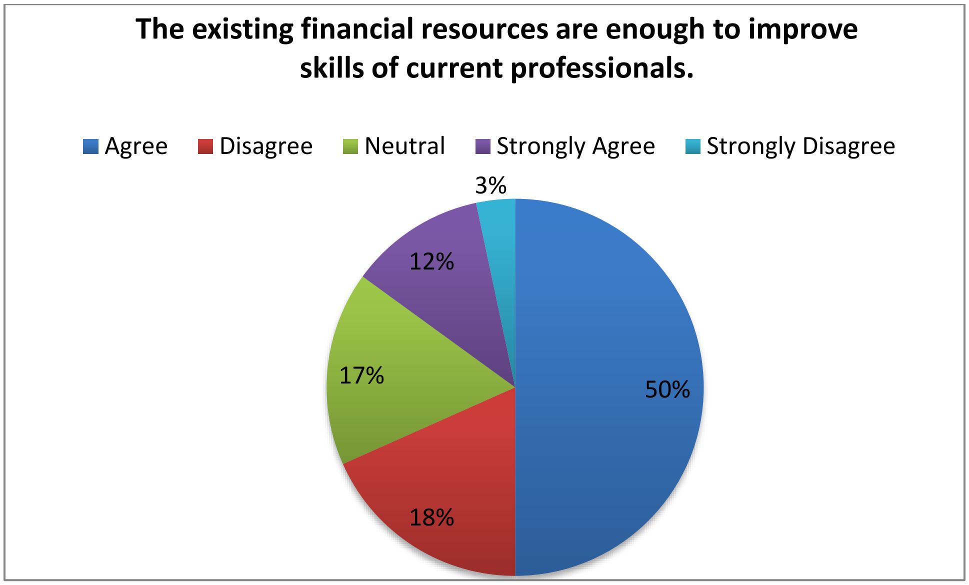

Figure 12. Financial resources to improve cyber security skills.

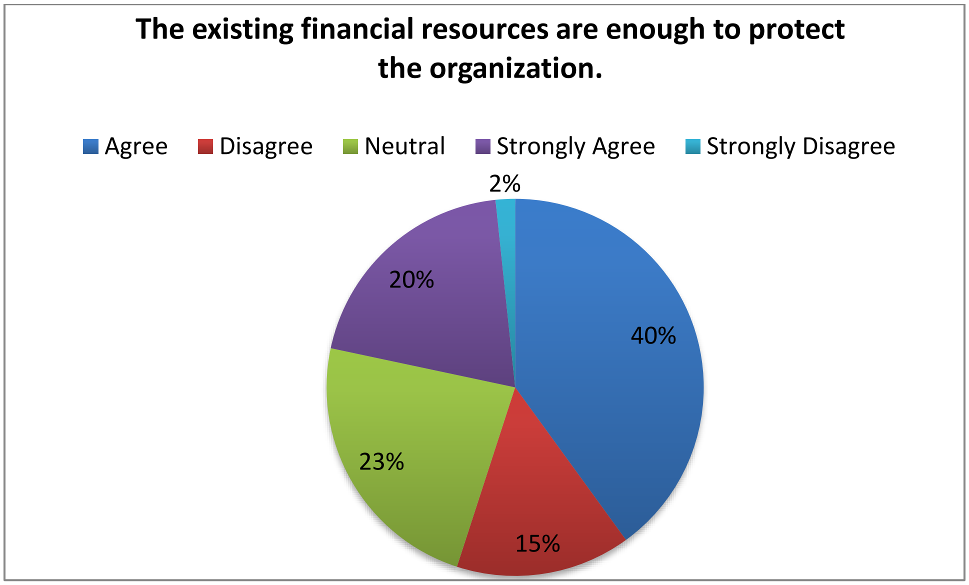

Figure 13. Financial resources to protect organization.

4. Awareness and education. Awareness is a learning procedure that sets the ground for training by changing personal and organizational attitudes to accomplish the importance of security and the unfortunate consequences of its failure. This is explicitly required in all aspects of life. Awareness is extremely important in the ICT security sphere, because a person's actions can affect an entire organization. Lack of awareness from the person responsible can cause serious damage and loss to an organization. Cyber security awareness is all about conveying information and best practices to specific target groups.

Cyber security awareness programs address how and what sorts of materials and tools can be used to convey messages and that make such programs successful and impactful or failures. It is the multidimensional structure of an awareness program itself that makes people interpret it differently at various levels. Therefore, understanding what constitutes effective cyber security awareness is imperative.

A more holistic way of describing cyber security awareness would be useful to attain effective cyber security awareness programs. A common understanding of this term is important to better comprehend what constitutes cyber security awareness. Enhancing cyber security awareness is a major goal for many organizations, whereby greater awareness of the state of environments enables improved decision-making [54].

40% of the experts agree that employees know how to protect themselves online; however, in 35% of the organizations users do not have enough knowledge in the field cyber security. The indices show that employees participate in security training courses just in 29% of organizations; on the other hand, 78.3% of experts agree that employees need regular awareness information on cyber threats.

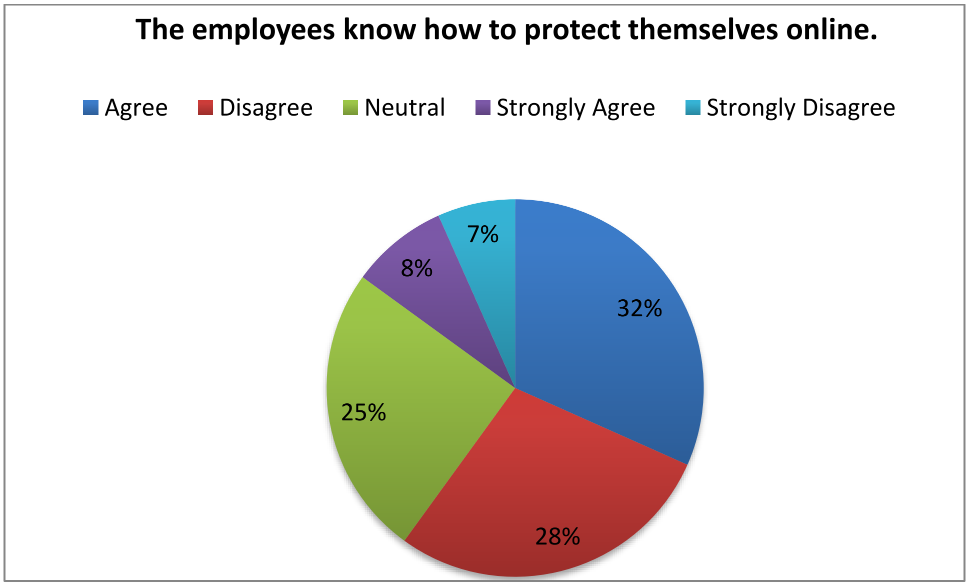

Figure 14. The employees know how to protect themselves online.

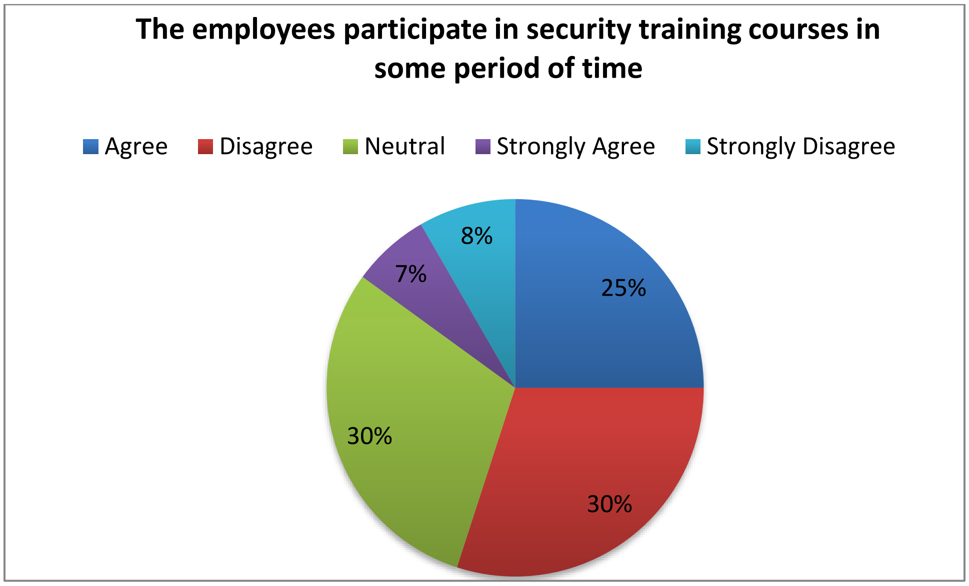

Figure 15. The employees' participation in security training courses.

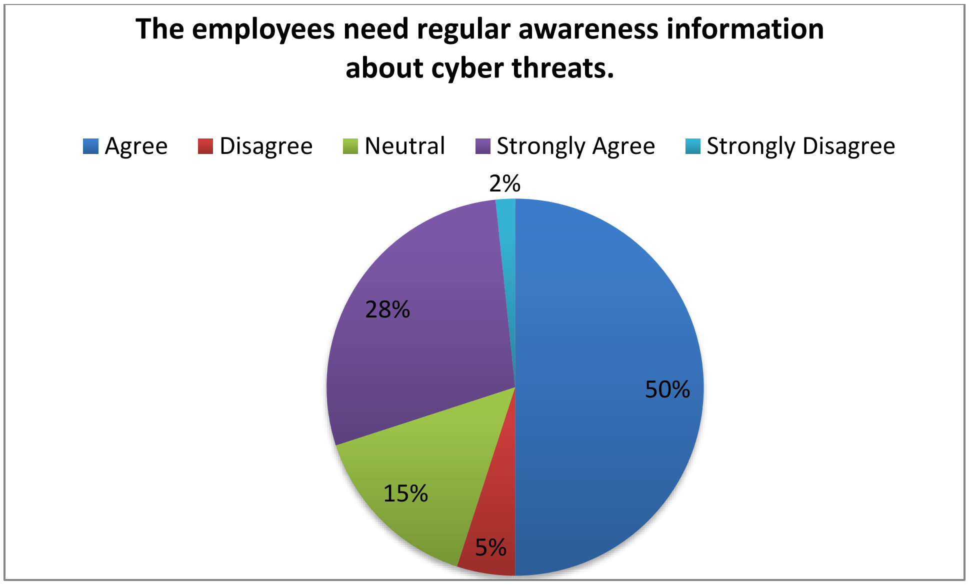

Figure 16.The employees' need regular awareness information.

5. Public-private cooperation. To understand the full picture of cyber security and cooperation among stakeholders, it is important to look at how small and medium-sized enterprises (SMEs) are involved in overall cyber security of the country. As mentioned earlier, their cyber security capabilities are only limited to their IT departments, and the government treats cooperation with them on cyber security the same as it would treat participation in any other sector which does not carry the same importance for the state and society overall [50]. The partnership between security agencies is vital because the jurisdictions have restricted boundaries related territory; however, cyberspace has not such boundaries. It's hard to attribute responsibility, both for the lack of reference paradigms and difficulty to monitor cyber events [55].

The survey responses show that 68.3% of the organizations have enough cooperation with public/private sector and 43.3% of these organizations are satisfied with sharing information with public/private sector. In 48.4% of the organizations employees know how to use the security related software bought from other companies.

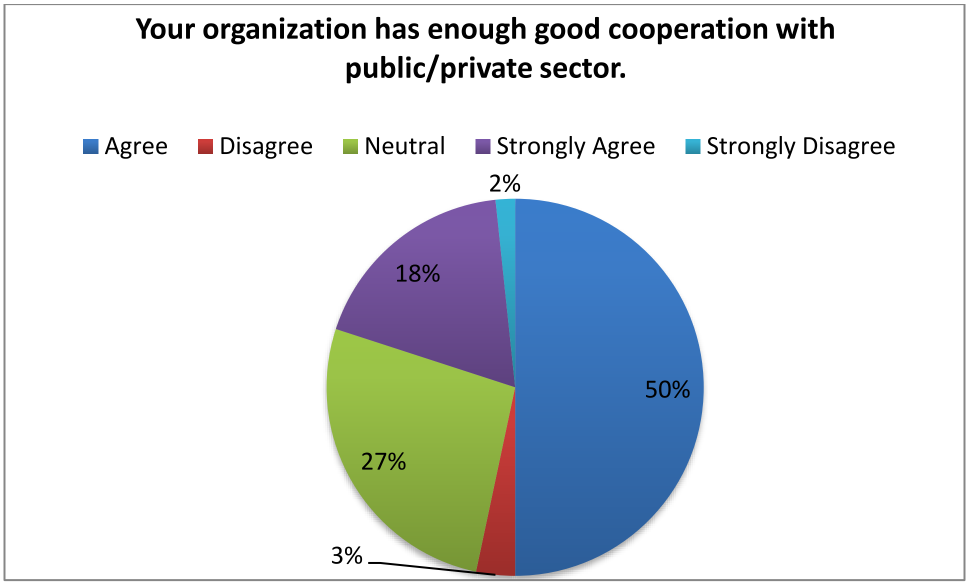

Figure 17. Cooperation with public/private sector.

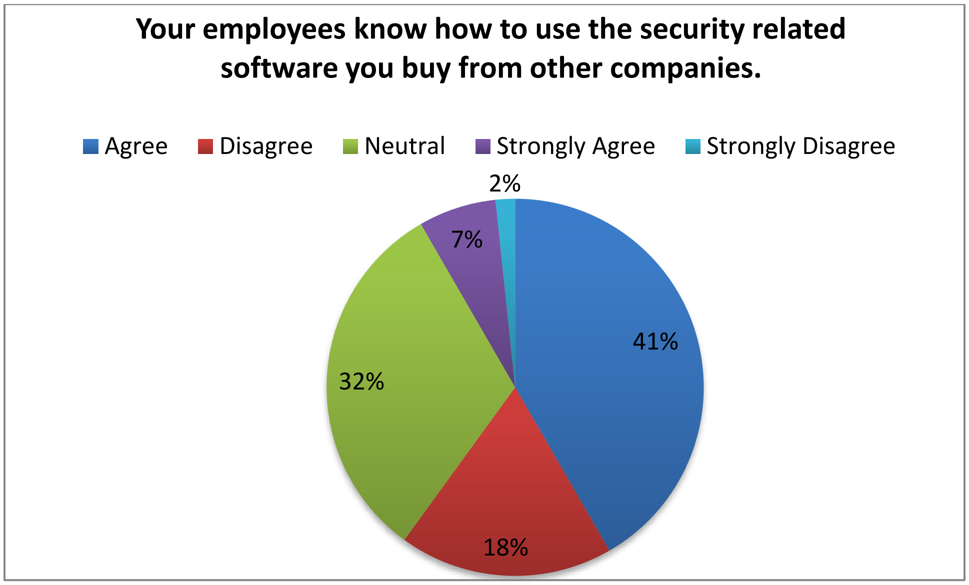

Figure 18. Employees' knowledge about security related software.

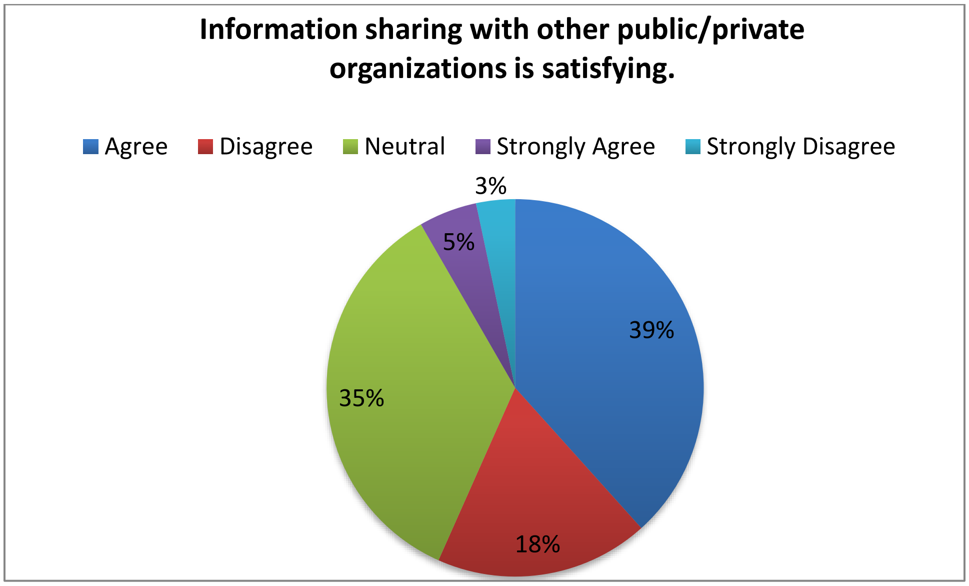

Figure 19. Information sharing.

6. Human recourses. Increasing the role information, information resources and technology in state's, society's and citizens' lives brings information security issues to the forefront. In this regard, there is a great demand for educated and skilled professionals in this area to protect the information security system, the system-related information resources and the users who use these technologies, and effectively fight against cyber crime. According to this, human resources is becoming the most important factor in CSCB. The role of human resources is becoming more responsible in CSCB: hiring skilled professionals; organizing programs to raise cyber security education and skills of existing experts; motivating employees to gain international cyber security certificates. Hence, organizations are faced with several issues related to this factor in Azerbaijan.

51.7% of the participants agree that there is lack of cyber security professionals in the organizations and especially in public sector which is more important in terms of critical infrastructure. There is enough number of professionals in just 23.3% of organizations in Azerbaijan and mostly these are private companies.

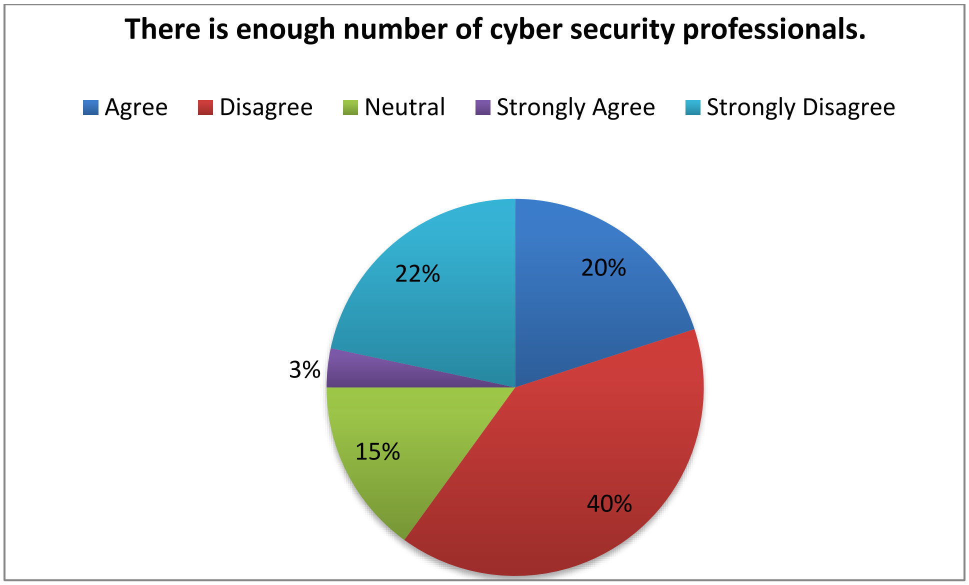

Figure 20. There is enough number of cyber security professionals.

Moreover, just 20% of the cyber security professionals are certified under the internationally recognized certification programs and 58.4% of experts have no any international certificate.

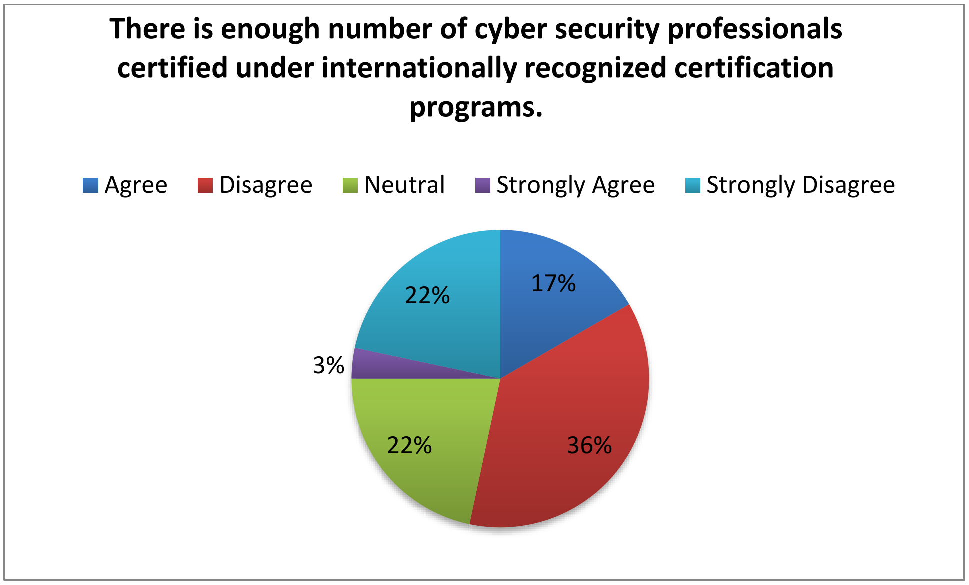

Figure 21. Certified cyber security professionals.

In 43.7% of organizations experts have no sufficient education level and just 28.4% of professionals have education in the field of cyber security.

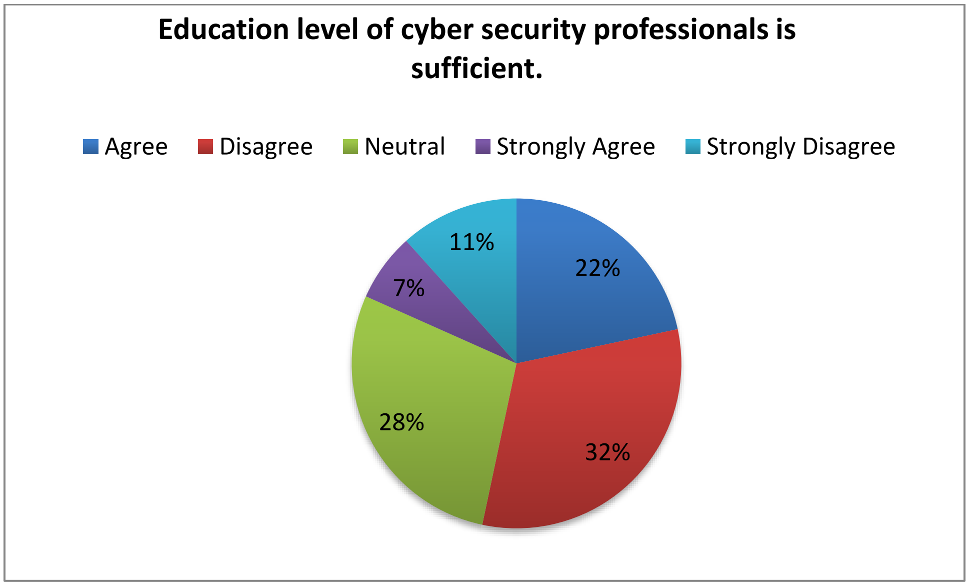

Figure 22. Education level of cyber security professionals is sufficient.

7. Education programs. As cyber crime has intensified in both scale and sophistication, education system has struggled to keep up. In recent years, there is a great demand in creation and development of undergraduate and graduate programs in terms of educating qualified specialists and increasing academic education. Organization and submission of both technical and legal educations at the university level should be a priority area in order to cover the lacks in cyber security area. Additionally, In order to provide solutions for the severe shortage in cyber security talent around the globe, cyber security education needs to be overhauled and women must be encouraged to enter this largely male dominated field.

Germany has several universities and institutes providing degrees and certificates in information security. The Federal Ministry of Education and Research funds the KASTEL competence center that offers training leading to a certificate equivalent to a specialized master degree in IT security. The Technical University of Darmstadt has been offering a Master of Science Degree in IT security since 2010. On the other hand, the UK and the US especially work on national education programs to improve cyber security in the country.

Unfortunately, it is different in Azerbaijan, hence local documents and experts prove that there is not enough number of university education programs in cyber security. Our research analysis indicates that 86.7% of the experts state the same idea, as well. Furthermore, they agree that the quality of current education is not satisfying and the national education programs are not enough for cyber security knowledge and career opportunities.

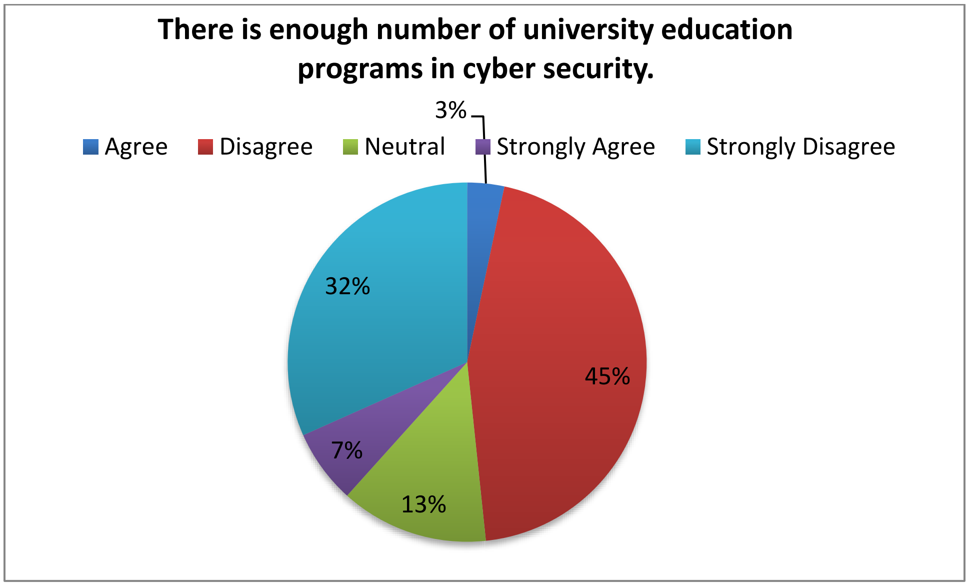

Figure 23. University education programs in cyber security.

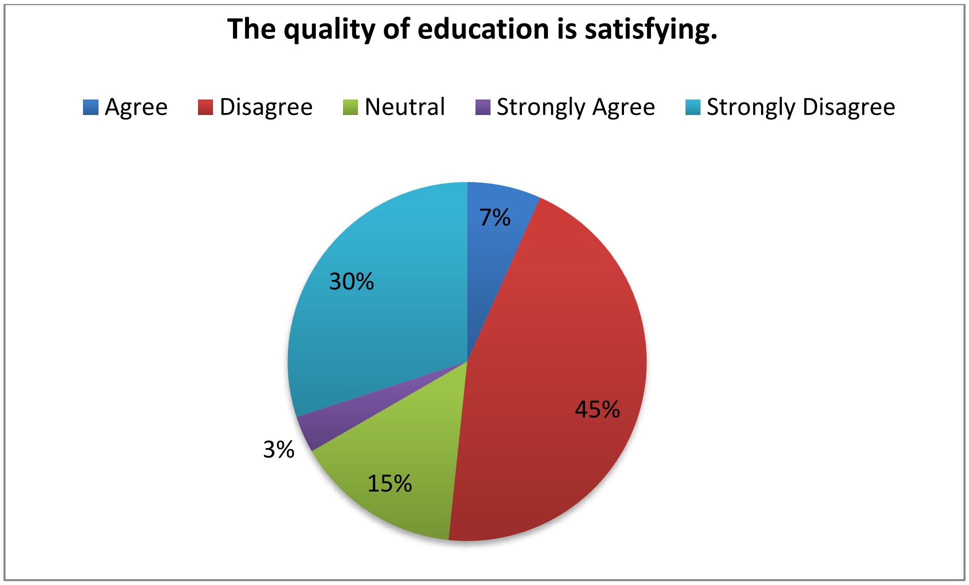

Figure 24. The quality of education.

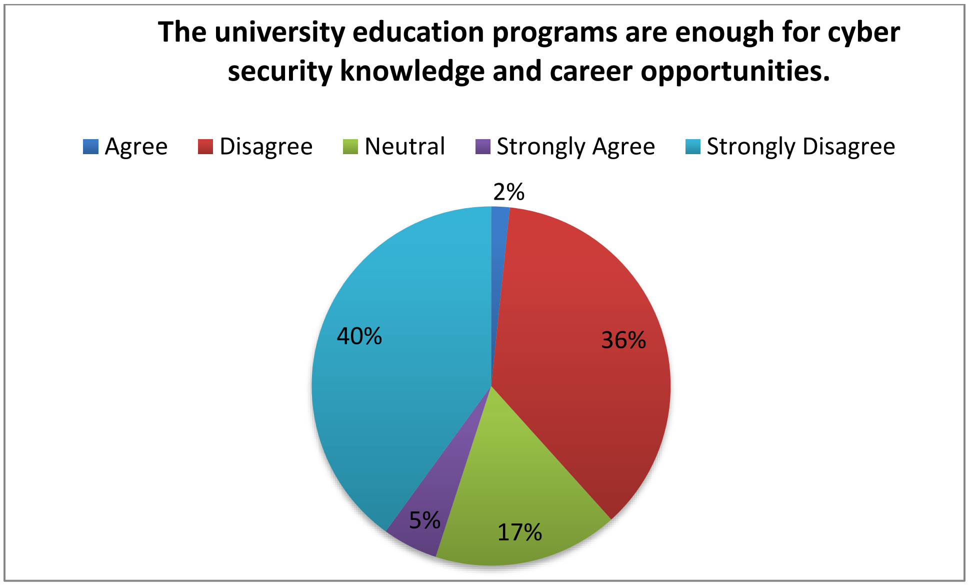

Figure 25. The university education programs for building cyber security career.

8. Training courses. As I mentioned above, the importance of education programs is increasing day by day, either the training courses at all levels becoming relevant as well. University degrees are flexible for specialists who want to start their education from earlier years. However, the training courses are more suitable for the experts who are currently working in the IT areas to gain more knowledge and improve existing skills.

While it is important that the strategy encourage improved cyber security skills and awareness in digital life at home, it must also encourage the development of a strong and cyber literate workforce.

Statistics from the survey data analysis results show that there is no enough number of training courses professionals in Azerbaijan; hence just 18.4% of responders disagree with this statement. 40% of the experts' state that the existing cyber security training courses are not enough to start career in cyber security. However, 23.3% of them disagree with this statement. Just 26.3% of the organizations provide financial support for the experts in participating on cyber security training courses.

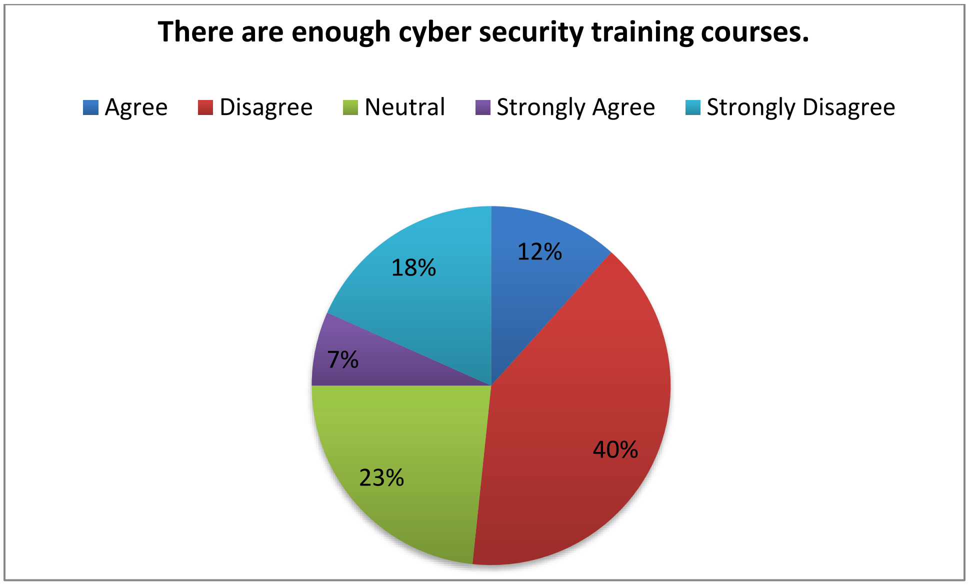

Figure 26. Cyber security training courses.

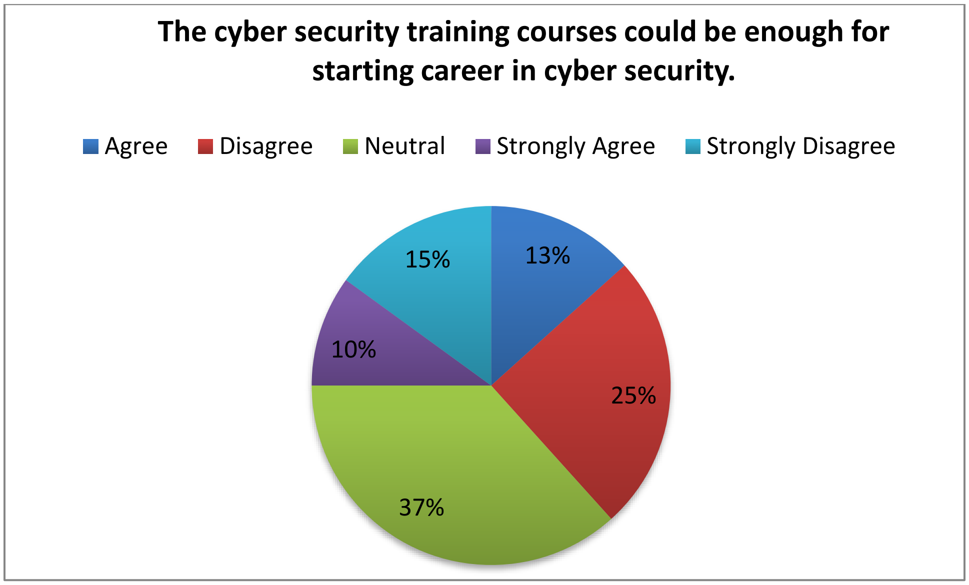

Figure 27. The training courses for building cyber security career.

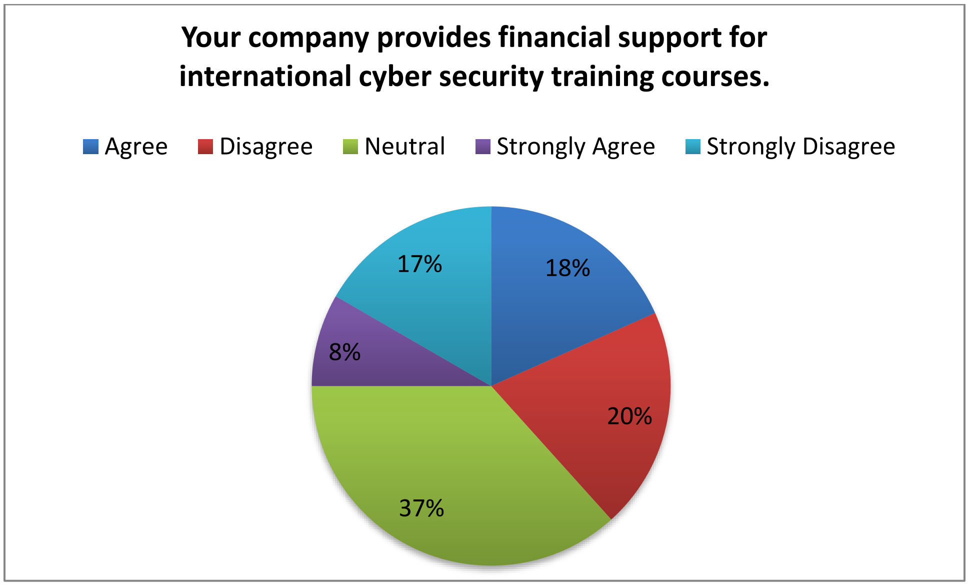

Figure 28. Financial support for international cyber security training courses.

9. Environment. Nowadays, the monitoring capabilities of information technologies and their providers are provoking a global crisis of confidence in both these technologies and the key players in the sector. In Azerbaijan as in the rest of the world, we are becoming increasingly aware of the fragility of digital environments, the fragility of confidence in techniques and actors in the field of cyber security. Systems, Internet of Things and Internet of Services, cyber incidents affecting those infrastructures have increased more than ever. Modern economies rely on the newly developed cyber infrastructures and assuring their security has become the top priority of many actors (governments, companies, etc.) as this may also be similar with protecting the economies or businesses [56].

Developing confidence in ICT infrastructures requires addressing and overcoming difficulties at many levels. These include the difficulty for individuals, organizations, and authorities in understanding threats, identifying risks, and implementing efficient and effective risk reduction measures, including the difficulty in unblocking sufficient means for combating cyber criminality.

Research analysis results indicate that just in 10% of the organizations technological environment is not sufficient for improving professionals' skills which means there is no lack of technological devices or tools to work and protect the organization against cyber threats. However, just 25% of the expert's state that technological environment in Azerbaijan is sufficient to build their career in the field of cyber security.

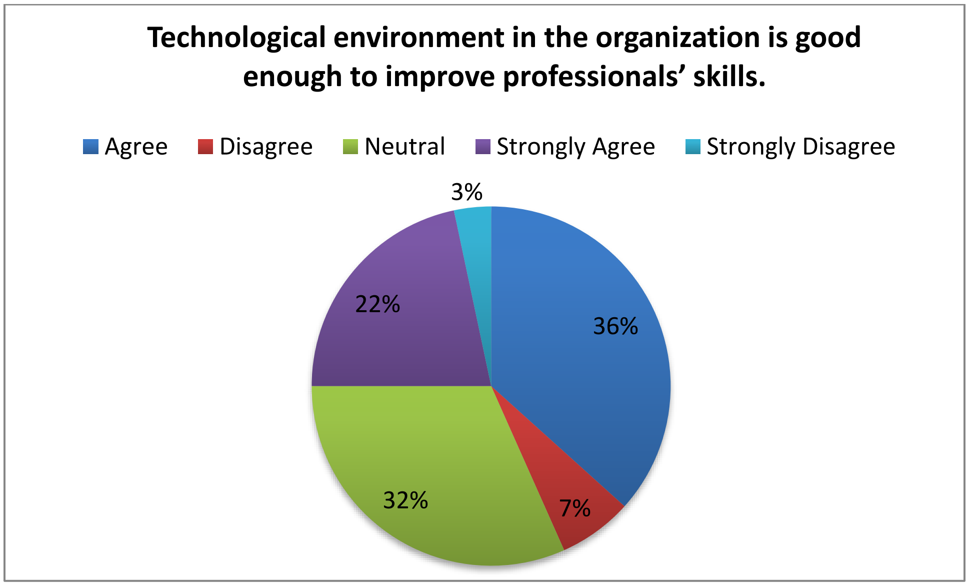

Figure 29. Technological environment.

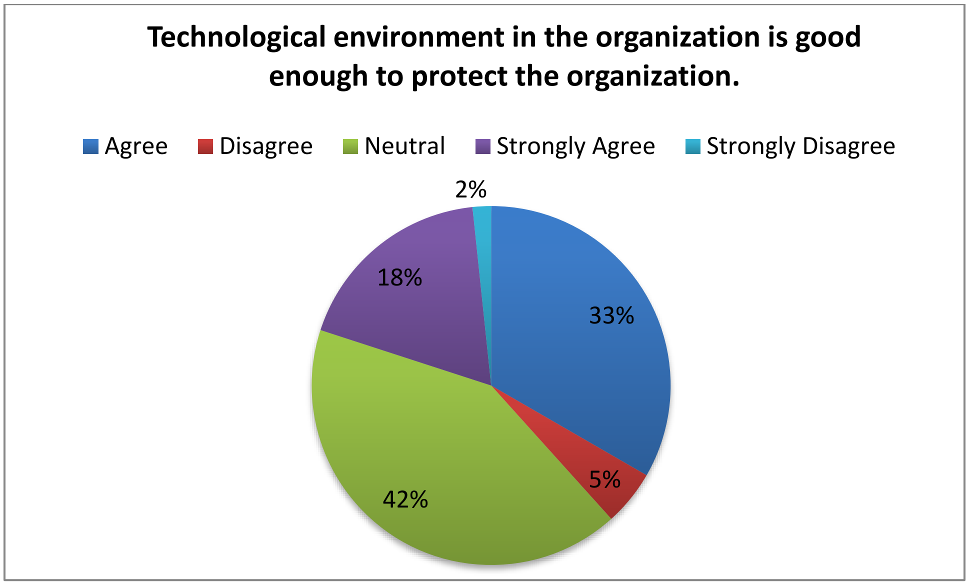

Figure 30. Technological environment is enough to protect the organization.

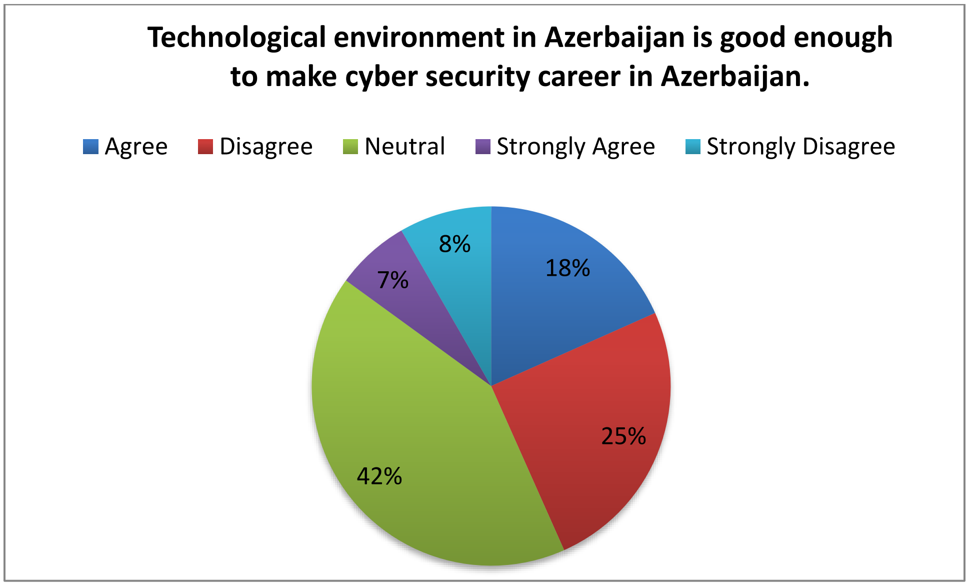

Figure 31. Technological environment is good enough to make cyber security career in Azerbaijan.

Chapter 4. Proposing Action Plan to solve cyber security capacity building challenges in Azerbaijan

4.1 Introduction

In this section, the author put forward an action plan for the solution of the problems of the CSCB in Azerbaijan. The action plan has divided into five dimensions, which discussed beforehand. In general, for the solution of problems related to cyber-threats, the preparation of the action plan was found in international practice. In the preparation of action plan is considered the best international practices and academic literature, combined with the analysis of situation in Azerbaijan in previous chapters. In the present situation, although some measures have been taken in the direction of CSCB in Azerbaijan, problems are still going on as it is not centralized and planned. The primary purpose of the thesis is to investigate these issues both locally and in a more detailed and precise manner based on the opinions of local experts and prepare an action plan accordingly. Five outreach activities are described in the next section considering all the facts mentioned above.

4.2 Action Plan

The process of implementation of the action plan involves the participation of various public and non-governmental stakeholders, as it was not prepared jointly with the government and therefore it creates some difficulties in determining responsible executive authorities and deadlines for each action. To increase the effectiveness of the action plan, it is necessary to phase this process down, mark the final deadline for each action, and assign the appropriate executive body as well as resources for implementation. Action plan was prepared according to the five dimensions and consists of 25 objectives and a possible list of actions of each objective. These action plans have been prepared depending on researching existing action plans in CSCB and national cyber security strategies of different countries and as well as various improvement solutions for CSCB [57] [9] [58] [10] [11] [59] [60]. Finally, the author analyzed these documents and compared internal experiences and existing situation in Azerbaijan. The action items provided are not exhaustive and should be amended according to the development of cyber security situation in Azerbaijan and internationally.

4.2.1. Cyber security Policy and Strategy

As shown in previous chapters, certain steps have been taken in the direction of developing cyber security policy and strategy in Azerbaijan. "National Strategy on the development of information society for 2014-2020" [7] and "2016-2020 State Program on the implementation of National Strategy for the development of information society" [20], "Azerbaijan 2020: Concept of Development" [21], and "Strategic Road Map for the development of communication and information technologies" [22] are the real examples. However, the increasing cyber threats and state-based attacks, show the importance to update and rewrite these policies and strategies according to the best practices used internationally.

The following table indicates total 5 actions and 29 sub-actions which have been defined based on previous analysis in cyber security strategy and policy in Azerbaijan.

Table 4. Action plan for Dimension 1 in Azerbaijan.

N	Action	Sub-action
1.	Developing new policies	- Define needs based on the current status - Formulate of policy documents - Implement a new policy - Adopt new policies - Evaluate policies - Terminate them based on evaluation results
2.	Development, publication, and dissemination of strategies	- Set objectives - Evaluate environment - Formulate a strategy document - Implement the strategy - Control the results
3.	Enhancing existing strategies	- Identify potential enhancement opportunity - Define actions - Implement of initiative or agreed actions - Discuss of findings and implications - Implement next actions - Embed of new practice/s - Monitor, Review, and Report
4.	Enhancing current policies	- Identify priority issues - Collect and analyze data

		- Improve policies based on analysis results - Draft policy proposals - Implement policies - Evaluate of policies
5.	Updating current guidelines	- Schedule updates - Full update of guidelines - Partial update of guidelines - Refresh the guidelines - Present updates

4.2.2. Cyber culture and society

At present, considerable improvements in the development of information society in Azerbaijan are noticeable. Providing electronic services for citizens, cooperation with foreign countries, increasing internet resources, etc. are filling this list. However, online security of citizens', especially children, developing national awareness programs, the creation of national search engine, and increasing capacity of national web content are the main challenges in this area. Government and organizations must take into account these circumstances and take action accordingly.

The following table indicates total 5 actions and 29 sub-actions which have been defined based on previous analysis in cyber culture and society in Azerbaijan.

Table 5. Action plan for Dimension 2 in Azerbaijan.

N	Objective	Action
1.	Awareness of citizens on cyber security	- Raise awareness amongst public and private organizations on the issues of cyber security and cybercrime and the importance of policy and legislation
2.	Developing national programs for awareness	- Develop, publish and disseminate a public awareness strategy - Develop a media campaign involving print & electronic media - Encourage companies to adopt cyber security awareness mechanisms as part of them - Corporate / Social Responsibility
3.	Taking measures on online child security	- Development and implementation of national programs on online child security - Create white and blacklists to protect children from existing threats - Implement filtered internet for children - Revise school curriculums to

		support/promote a cultural change
4.	Providing online security for citizens	- Develop and implement incident response procedure guidelines - Develop a Cyber Incident Management Framework - Develop a strategy that includes advertising, partnerships, web, social media, proactive media relations, earned media, political engagement, exhibits/special events, and internal communications plans.
5.	Promoting national preparedness	- Conduct training workshops and ensure maximum participation - Standardize basic components of training programs among institutions and customize, where necessary, according to how the country is structured

4.2.3. Cyber Security Education and Training

As shown in previous chapters, depending on analysis of local documents and expert survey, there are not any cyber security education at university level in Azerbaijan. Also, according to experts, the quality of education is deficient in many IT-related study programs at universities, and no education and training courses are available in cyber security. As we know, one of the key factors of development of cyber security is education and Azerbaijan is far behind it. Education is an important factor for the future development of cyber security in the country as well as training of experts. To raise knowledge and skill of experts the top activities, to be implemented in this area, are implementing university-level cyber security programs and, opening training centers. Moreover, employees in public and non-public sectors are required to be informed about cyber security awareness by the law.

The following table indicates total 5 actions and 29 sub-actions which have been defined based on previous analysis in cyber security education and training in Azerbaijan.

Table 6. Action plan for Dimension 3 in Azerbaijan.

N	Objective	Action
1.	Developing national cyber security education programs	- Establishment of an academic center of excellence focused specifically on cyber security - Establish a cyber security career awareness campaign targeting educators, students, parents, administrators, and counselors

		- Develop extra-curricular experiences (e.g., competitions, camps, clubs, boy/girl scouts, etc.) for youth that excite them about careers in cyber security and introduce them to the corresponding academic pathways.
2.	Developing education programs in universities on cyber security	- Include cyber security courses to the university curriculums - Infuse cyber security concepts into classroom instruction - Increase coordination among teacher preparation, professional development, support, and recognition efforts within existing and proposed cyber security educator programs - Stimulate innovative educational approaches to accelerate learning and skills development - Develop a nationally recognized cyber security career pathway for university students
3.	Preparing future cyber security workforce	- Increase the appeal of the cyber security profession to a diverse audience - Develop and replicating new programs that support youth obtaining knowledge, skills, and abilities required for success in the future cyber security workforce - Increase the number of youth pursuing cyber security or cyber security related degree, certificate or job - Develop a nationally recognized cyber security academic pathway for elementary, middle and secondary school students.
4.	Training employees at all levels in organizations	- Schedule training of employees - Plan training content for each level of employees - Train employees in different levels
5.	Enhancing professionals' skills in the field of cyber security	- Review of existing training initiatives in this area - Improve current training programs - Establish cyber security laboratories - Improve existing cyber security laboratories - Develop simulation systems for training of professionals

4.2.4. Legal and Regulatory Frameworks

With the new challenges arising in cyber space, the existing cyber security legislative system of Azerbaijan should periodically be renewed, and new legal solutions should be made in various areas. The protection of personal information, which is extremely important, does not have enough coverage in the Azerbaijani legislation. The EU General Data Protection Regulation (GDPR), which will enter into force on May 25 of the current year, is an important step in protecting the data of EU citizens. The integration of the GDPR into Azerbaijani legislature will solve this problem. The Budapest convention, in which is Azerbaijan member state, must be used in regulation the national fight against cyber crime. Moreover, there is lack of laws in online child pornography and protection of citizens' online rights in Azerbaijan.

The following table indicates total 5 actions and 29 sub-actions which have been defined based on previous analysis in cyber security legal and regulatory frameworks in Azerbaijan.

Table 7. Action plan for Dimension 4 in Azerbaijan.

N	Objective	Action
1.	Establishment of effective legislation which balances public safety with human rights, privacy, and data protection regimes	- Identify countries with existing legislation and use as a model for development - Utilize Budapest Convention as the basis for national cybercrime legislation
2.	Enactment of appropriate Cyber security legislation	- Develop and review existing draft legislation - Countries which have enacted law can also be used as models and assistance
3.	Develop a mechanism and infrastructure for dealing with online child pornography	- Develop the appropriate legislation - Develop and adopt a national or regional online reporting mechanism - Develop appropriate response mechanism
4.	Developing new frameworks for public-private partnership	- Preparing new mechanisms for effective public-private collaboration - Develop and implement information sharing arrangements and protocol - Developing a new process for public-private partnership - Develop a national partnership program

4.2.5. Standards, Organizations, and Technologies

Following the analysis of expert survey and the analysis of the current infrastructure, there are sufficient technological environment and financial resources for the development and management of cyber security in Azerbaijan. However, not every organization in the country uses available capabilities and, therefore, it is necessary to organize a mandatory cyber security team and infrastructure for each organization. International standards has to be applied to each organization and international experience for its implementation should be taken advantage of. Additionally, there is a need to increase the potential of CERT Azerbaijan and arrange close cooperation with state and non-state agencies.

The following table indicates total 5 actions and 29 sub-actions which have been defined based on previous analysis in cyber security standard, technologies and organizations in Azerbaijan.

Table 8. Action plan for Dimension 5 in Azerbaijan.

N	Objective	Action
1.	Implementation of international standards	- Ensure that networks are correctly configured and that the appropriate infrastructure is used - Adopt and comply with ISO Standards (including training) - Adopt a top-down approach to policy development and include civil society and the internet society in setting standards
2.	Building cyber security teams in organizations	- Define at least one cyber security officer in the organization - Clear roles and responsibilities - Identify needs for the officer' efficient work
3.	Developing cyber security infrastructure in organizations	- Develop policies and procedures to facilitate the effective detection, diagnosis, remedying and review of cyber attacks - Build monitoring systems - Update of cyber security software licenses - Increase the number of cyber security labs available - Train in the use of cyber security software
5.	Supporting innovations in cyber security	- Invest in research and development - Support start-ups on cyber security
6.	Increase existing capacity of CERTs	- Request assistance from international partners to establish CERT at the national level

Chapter 5. Future work

The study, being of an exploratory and interpretive nature, raises some opportunities for future research, both regarding theory development and concept validation. More research will, in fact, be necessary to refine and further elaborate our novel findings.

First, some new and useful conceptual categories have been generated given the in-depth action plan focused on CSCB. The study could thus be extended in search of statistical, rather than analytical, generalizability, as has been sought here.

Second, the study offers an opportunity to refine and validate the concepts and constructs that emerged from inductive analysis. The model discussed in above sections could also be used to generate some hypotheses for further research. The study could also be extended in longitudinal and comparative ways.

Further research could elaborate on this point, providing precious information to selection panels and training bodies. Future research could also take a historical perspective and ask if the current status of information security has significantly changed in the last several decades.

Finally, as was discussed before, further work is necessary to examine the best practices of other countries on national cyber security development, as we have done here. Future research can thus shed light on the dynamics of CSCB, information sharing and exchange among the particular group of individuals, state organizations, and governments.

The author believes that there are likely to be much more ongoing research projects in the cyber security capacity building field in Azerbaijan shortly.

In the future, given the further improvement of this thesis, it will may be beneficial and productive to divide the proposed action plan among relevant agencies in Azerbaijan and to coordinate with various public and non-governmental bodies.

Later on, it is crucial that following international experience and the current capacity of Azerbaijan the timeline for each event and the stages should be separated.

6. Conclusion

The purpose of the thesis has been to propose action plan in CSCB in Azerbaijan based on five dimensions:

- Cybersecurity Policy and Strategy
- Cyber Culture and Society
- Cybersecurity Education, Training and Skills
- Legal and Regulatory Frameworks
- Standards, Organizations, and Technologies

To achieve the purpose, the author has analyzed various Azerbaijani documents related to cyber security and conducted a survey among IT and Cyber Security professionals in Azerbaijan, in order to define existing challenges in CSCB. The analysis existing situation in CSCB in Azerbaijan and preparation action plan have been done in cooperation with CERT Azerbaijan.

The author has focused on five main directions in the research and in providing practical solution of the CSCB in Azerbaijan. The effectiveness of the model which has been developed and applied worldwide by the GCSCC, can be seen in real-life experiences [61]. CERT Azerbaijan provided valuable input in the conduct of analysis as well as in discussing the proposals.

As a result of research, it has been established that there are problems with the CSCB in Azerbaijan, and more specifically, some specific areas (Education and Training in Cyber Security) have not been developed yet, and relevant steps have been taken in some areas (Cyber Security Environment). An action plan was designed for the solution and development of the CSCB in Azerbaijan considering all the facts into account. To achieve a goal, the action plan is absolute. State agencies in Azerbaijan do not start any activity without an action plan - for example, CERT Azerbaijan should provide an action plan if it wants to operate by its statute. Upon receipt of a confirmation from the Cabinet of Ministers, the work must be continued according to the project and should provide the year-end report according to the plan. From this point of view, the preparation and implementation of the action plan is a practical state-level step for Azerbaijan.

The author believes that this plan will improve the situation in the CSCB and help to eliminate existing problems. However, one major constraint in this work was the lack of time, and lack of cyber security professionals in the country. Despite all this, the action plan has been developed and could be used as a basis to develop CSCB.

Bibliography

[1] MFA Azerbaijan, "Co-operation with international organizations," 2017. [Online]. Available: http://www.mfa.gov.az/content/737. [Accessed February 2018].

[2] M. Banks, "MEPs call for complete rethink of eastern neighbourhood partnership policy," April 2016. [Online]. Available: https://www.theparliamentmagazine.eu/articles/news/meps-call-complete-rethink-eastern-neighbourhood-partnership-policy. [Accessed February 2018].

[3] WEF, "The future of Azerbaijan's economy," January 2016. [Online]. Available: https://www.weforum.org/agenda/2016/01/azerbaijan/. [Accessed February 2018].

[4] EBRD, "Azerbaijan. European Bank for Reconstruction and Development.," 2015.

[5] CAERC, "Azerbaijan ranks first among CIS countries according to the rating of the World Economic Forum," January 2017. [Online]. Available: http://ereforms.org/news/azerbaijan_ranks_first_among_cis_countries_according_to_the_rating_of_the_world_economic_forum-71. [Accessed February 2018].

[6] K. Schwab, "The Global Competitiveness Report 2016–2017.World Economic Forum," 2017.

[7] The Republic of Azerbaijan, "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiyanın təsdiq edilməsi," 2014. [Online]. Available: http://www.e-qanun.az/framework/27456. [Accessed March 2018].

[8] GCSCC, 2018. [Online]. Available: https://www.oxfordmartin.ox.ac.uk/cybersecurity. [Accessed February 2018].

[9] Lilly Pijnenburg Muller, "Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities," March 2015. [Online]. Available: https://brage.bibsys.no/xmlui/bitstream/id/331398/NUPI+Report+03-15-Muller.pdf. [Accessed April 2018].

[10] Government of Canada, "Action Plan 2010-2015 for Canada’s Cyber Security Strategy," 2013. [Online]. Available: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ctn-pln-cbr-scrt/index-en.aspx. [Accessed April 2018].

[11] Australian Government, "CYBER SECURITY STRATEGY ACTION PLAN," 2017. [Online]. Available: https://cybersecuritystrategy.pmc.gov.au/action-plan/index.html. [Accessed April 2018].

[12] B. Chia-Chien, "The Delphi Technique: Making Sense of Consensus," 2017.

[13] H. &. Murray, "The Delphi Method: Techniques and Applications.," 2002.

[14] GCSCC, "Cybersecurity Capacity Maturity Model for Nations (CMM)," February 2017. [Online]. Available: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0. [Accessed April 2018].

[15] Я. Ом, "Киберкультура Cyberculture," August 2009. [Online]. Available: https://www.proza.ru/2009/08/28/1077. [Accessed April 2018].

[16] MinCom, "Information Society," [Online]. Available: http://www.mincom.gov.az/activity/information-technologies/information-society/. [Accessed February 2018].

[17] G. &. Nicholas, "Developing a National Strategy for Cybersecurity.," 2013.

[18] Organisation for Economic Co-Operation and Development, "Cybersecurity Policy Making at a Turning Point. Analysing a new generation of national cybersecurity strategies for the Internet economy," 2012. [Online]. Available: https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf. [Accessed February 2018].

[19] The Republic of Azerbaijan, "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiyanın təsdiq edilməsi," April 2014. [Online]. Available: http://www.e-qanun.az/framework/27456. [Accessed February 2018].

[20] The Republic of Azerbaijan, "State Program on the implementation of the National Strategy for Information Society Development in Azerbaijan for 2016-2020 years," September 2016. [Online]. Available: http://www.mincom.gov.az/legislation/orders/. [Accessed April 2018].

[21] The Republic of Azerbaijan, "“AZERBAIJAN 2020: LOOK INTO THE FUTURE” CONCEPT OF DEVELOPMENT," [Online]. Available: https://www.president.az/files/future_en.pdf. [Accessed April 2018].

[22] The Republic of Azerbaijan, "Azərbaycan Respublikasında telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi," 2016. [Online]. [Accessed February 2018].

[23] N. Orujova, "Information Society Strategy to be implemented in two stages.," April 2014. [Online]. Available: https://www.azernews.az/business/65843.html. [Accessed February 2018].

[24] EU/CoE Eastern Partnership Facility, "Cybercrime and cybersecurity strategies in the Eastern Partnership region," *CyberCrime@EAP,* pp. 19-22, 2014.

[25] The Republic of Azerbaijan, "Azərbaycan Respublikasında telekommunikasiya və informasiya texnologiyalarının inkişafına dair Strateji Yol Xəritəsi," 2016. [Online]. Available: http://ictfund.gov.az/wpcontent/uploads/2016/10/IKT_strateji_yol_xeritesi.pdf. [Accessed February 2018].

[26] The Republic of Azerbaijan, "İnformasiya təhlükəsizliyi sahəsində fəaliyyətin təkmilləşdirilməsi tədbirləri haqqında," 2012. [Online]. Available: www.e-qanun.az/framework/24353. [Accessed February 2018].

[27] А. М. Блюмин, Н. А. Феоктистов, "Роль и значение информационных ресурсов в развитии информационных технологий и в информатизации общества," 2010. [Online]. Available: http://scibook.net/informatsionnyie-tehnologii_1237/rol-znachenie-informatsionnyih-resursov-41723.html. [Accessed April 2018].

[28] The Republic of Azerbaijan, "Hüquqi Sənədlər," [Online]. Available: https://cert.gov.az/az/documents. [Accessed January 2018].

[29] MinCoM, "İLLİK HESABAT 2014," 2014. [Online]. Available: http://mincom.gov.az/assets/pdf/HESABAT_2014.pdf. [Accessed March 2018].

[30] MinCoM, "E-Hökumət," [Online]. Available: http://www.mincom.gov.az/fealiyyet/it/e-gov/. [Accessed March 2018].

[31] K.Zərbalıyeva, "Azərbaycan və Estoniya arasında informasiya və kommunikasiya texnologiyaları sahəsində əməkdaşlığa dair saziş imzalanıb," 2009. [Online]. Available: https://az.trend.az/azerbaijan/politics/1546006.html. [Accessed April 2018].

[32] Trend news agency, "Estonia's Digital Revolution Takes Root in Azerbaijan," August 2014. [Online]. Available: https://en.trend.az/business/economy/2306150.html [. [Accessed March 2018].

[33] Asanimza.az, "Asan İmza – your identification," [Online]. Available: http://asanimza.az/asan-imza-in-english/. [Accessed February 2018].

[34] Manevr.az, "Azərbaycanın müdafiəsi üçün kiber əsgərlər yetişdirmək lazımdır," December 2016. [Online]. Available: http://manevr.az/elm-tehsil/6160-azerbaycanin-mudafiesi-uchun-kiber-esgerler-yetishdirmek-lazimdir.html. [Accessed April 2018].

[35] Ministry of Education Republic of Azerbaijan, "Təhsil müəssisələri," [Online]. Available: http://edu.gov.az/az/page/339. [Accessed March 2018].

[36] itstep.az, "IT Step Academy," [Online]. Available: https://itstep.az/academy/. [Accessed March 2018].

[37] itstep.az, "Təhsil formaları," [Online]. Available: https://itstep.az/t%c9%99hsil-formalari/. [Accessed April 2018].

[38] code.edu.az, "TƏDRİS PROQRAMLARIMIZ," [Online]. Available: https://code.edu.az/. [Accessed April 2018].

[39] C. o. Europe, " Law of the Republic of Azerbaijan on approval of Convention “On Cybercrime”," September 2009. [Online]. Available: http://www.mincom.gov.az/legislation/laws/. [Accessed April 2018].

[40] The Republic of Azerbaijan, "Criminal Code," 2012. [Online]. Available: http://www.e-qanun.az/code/11. [Accessed March 2018].

[41] The Republic of Azerbaijan, "On Ensuring the activities of the Electronic Security Center under the Ministry of Communications and Information Technologies of the Republic of Azerbaijan," March 2013. [Online]. Available: http://www.mincom.gov.az/legislation/decrees/. [Accessed April 2018].

[42] AzStand, "Reports on Activities of the Technical Committee on Standardization of Information and Communications Technology," 2009. [Online]. Available: http://www.azstand.gov.az/index.php?lang=3&id=179. [Accessed March 2018].

[43] ITU, "Cyberwellness Profile: Azerbaijan," 20014.

[44] Makili-Aliyev, K., & Rehman, A., "Cyber-Security Objective: Azerbaijan in the Digitalized World," Vols. SAM Review , 11, pp. 5-27, 2013.

[45] News.az, "Baku and Moscow Start Joint Closure of Extremist and Criminal Sites, Proviers," 2012. [Online]. Available: http://news.az/articles/society/53592. [Accessed April 2018].

[46] Mission of Azerbaijan to NATO, "20 Years of Azerbaijan-NATO Partnership. Brussels: Mission ofAzerbaijan to NATO," 2014.

[47] J. Clough, "Principles of Cybercrime," Cambridge: Cambridge University Press, 2010.

[48] AzNet, "Internet Access and Infrastructure Development for research, educational and civil society development purposes," 2005. [Online]. Available: https://tnc2005.terena.org/core/getfilea592.pdf?file_id=537. [Accessed April 2018].

[49] International Finance Corporation, "Study of Small and Medium," 2009. [Online]. Available: https://www.ifc.org/wps/wcm/connect/75675a804a1d4d8390d19c02f96b8a3d/eng-

final.pdf?MOD=AJPERES&CACHEID=75675a804a1d4d8390d19c02f96b8a3d. [Accessed April 2018].

[50] ITU, "The Quest for Cyber Confidence," 2014.

[51] Cyber Security Center, "CERT.AZ description as per RfC 2350," 2014.

[52] Cyber Security Center, "Regulation," 2017. [Online]. Available: https://www.cert.az/en/regulation.html. [Accessed April 2018].

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

[54] Zahri Yunos, Ramona Susanty Ab Hamid, Mustaffa Ahmad, "Development of a cyber security awareness strategy using focus group discussion," in *SAI Computing Conference*, 2016.

[55] OECD, "Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies," OECD Digital Economy Papers No.212, 2012.

[56] Tofan, D., Nikolakopoulos, T., & Eleni, D., "The cost of incidents affecting CIIs," 2016. [Online]. Available: https://doi.org/10.2824/475621. [Accessed April 2018].

[57] Caricom, "CARICOM Cyber Security and Cybercrime Action Plan," March 2016. [Online]. Available: http://thecommonwealth.org/sites/default/files/news-items/documents/6%20FinalCastriesDeclaration170316.pdf. [Accessed April 2018].

[58] European University Association asbl, "IMPROVING QUALITY,ENHANCING CREATIVITY: CHANGE PROCESSES IN EUROPEAN HIGHER EDUCATION INSTITUTIONS," 2009. [Online]. Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiAsuCWxc7aAhUlDZoKHUAaArkQFggsMAA&url=http%3A%2F%2Fwww.eua.be%2Ftypo3conf%2Fext%2Fbzb_securelink%2FpushFile.php%3Fcuid%3D400%26file%3Dfileadmin%2Fuser_upload%2Ffiles%2FPublications. [Accessed April 2018].

[59] Inter-American Development Bank (IDB) & Organization of American States, "Cybersecurity Are We Ready in Latin America and the Caribbean?," www.cybersecurityobservatory.com, 2016.

[60] REPUBLIC OF KOSOVO, "National Cyber Security Strategy and Action Plan 2016 – 2019," March 2015. [Online]. Available: http://www.kryeministri-ks.net/repository/docs/National_Cyber_Security_Strategy_and_Action_Plan_2016-2019_per_publikim_1202.pdf. [Accessed April 2018].

[61] GCSCC, "Our aim is to understand how to deliver effective cyber security both within the UK and internationally.," 2017. [Online]. Available: https://www.oxfordmartin.ox.ac.uk/cybersecurity. [Accessed April 2018].

[62] ITU, "Global Cybersecurity Index (GCI) 2017," 2017.

Appendix 1 - Questionnaire on Defining cyber security capacity building problematic factors in Azerbaijan

1. Introduction.

The study will attempt to check the current situation of education in cyber security in Azerbaijan. The study intends to collect data from Cyber Security Specialists, IT Experts and other professionals working in public and private sectors in information technology areas. Link to questionnaire:
https://docs.google.com/forms/d/e/1FAIpQLSc9Iomstu6jqWNZu-7BAu5HxeEc8dGhAkzISInOlpou1rJUMQ/viewform

I will be grateful if you would take a moment to complete this survey. Participation in this survey is voluntary and information provided will be used only for the purpose of this study and will be treated with the strictest of confidence. I thank you in advance for giving your valuable time to answer the questionnaire.

In case of questions or comments please contact Javid Asadli: jaasad@ttu.ee

2. Identification (General information about the participants).

1. What is your position in information technology?

   a) Expert on Cyber Security

   b) Other Information Technology Professionals

2. Job type:

   a) Public sector

   b) Private sector

3. What is your current age group?

a) 18-24

b) 25-34

c) 35-54

d) 55 or older

4. What is your current experience group?

a) Less than 1 year

b) 1-3 years

c) 3-5 years

d) More than 5 years

3. Stability (Structure and institutional stability that can allow for utilization of the Internet, while simultaneously guarding the users against malware threats, which increase with access to cyberspace.)

1) The existing capacity in your organization is enough to build a cyber security team.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

2) The cyber security knowledge of current professionals is enough to protect your organization.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

3) Decision makers or responsible people in your organization know the needs to improve cyber capacity.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

4. Legislation (An adequate legislative framework that can enact decisions for building a secure cyberspace.)

1) There is cyber security policy of organization.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

2) The existing legislative frameworks of the organization are enough for building cyber security capacity.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

3) There is enough number of guidelines for building cyber security in your organization.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

5. Resources (Resources to build what the organization need to construct and secure capacities in cyberspace)

1) The existing financial resources are enough to build capacity.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

2) The existing financial resources are enough to improve skills of current professionals.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

3) The existing financial resources are enough to protect the organization.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

6. Awareness and education (Education about the threats and risks that come with cyberspace in today's world of escalating use of cyberspace through increased access)

1) The employees know how to protect themselves online.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

2) The employees participate in security training courses in some period of time

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

3) The employees need regular awareness information about cyber threats.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

7. Public-private cooperation (Public-private partnership models need to be created in the country building its cyber capacities as the private industry owns much of the ICT infrastructure and is most active in the development of new technologies)

1) Your organization has enough good cooperation with public/private sector.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

2) Your employees know how to use the security related software you buy from other companies.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

3) Information sharing with other public/private organizations is satisfying.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

8. Human Resources (Existing human resources, enhancing skills of professionals, preparing new professionals)

1) There is enough number of cyber security professionals.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

2) There is enough number of cyber security professionals certified under internationally recognized certification programs.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

3) Education level of cyber security professionals is sufficient.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

9. Education programs (Current education programs to prepare new professionals in the field of cyber security)

1) There is enough number of university education programs in cyber security.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

2) The quality of education is satisfying.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

3) The university education programs are enough for cyber security knowledge and career opportunities.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

10. Training courses (Training is needed, in the form of awareness creation and technical education in the field of cyberspace and security)

1) There are enough cyber security training courses.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

2) The cyber security training courses could be enough for starting career in cyber security.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

3) Your company provides financial support for international cyber security training courses.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

11. Environment (The need to build the correct environment for technology)

1) Technological environment in the organization is good enough to improve professionals' skills.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

2) Technological environment in the organization is good enough to protect the organization.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree

3) Technological environment in Azerbaijan is good enough to make cyber security Career in Azerbaijan.

a) Strongly Agree

b) Agree

c) Neutral

d) Disagree

e) Strongly disagree