TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Ilkin Huseynov 184595IVCM

THE ANALYSIS OF THE CURRENT CYBER SECURITY ACTIONS TAKEN IN THE E-GOVERNMENT OF AZERBAIJAN AND PROPOSAL OF THE IMPROVEMENT PLAN

Master’s thesis

Supervisor: Mika Juha Kerttunen
PhD

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Ilkin Huseynov 184595IVCM

ASERBAIDŽAANI E-VALITSUSE KÜBER TURBE TEGEVUSTE ANALÜÜS JA PARENDUS ETTEPANEKUD

Magistritöö

Juhendaja: Mika Juha Kerttunen
PhD

Tallinn 2020

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: Ilkin Huseynov

04.08.2020

Abstract

With the rising importance of cyber security in the state practices after the initiation of E-Government system, Azerbaijani government tries to find the best policy solutions to secure the data of its citizens without compromising the intrastate agency communication. Therefore, this research study aims at finding the crucial problems within the governmental policies and assess the best policy choices for that. Study involves the qualitative research methods as it performs background analysis of the roots of the problem and takes interview from 2 cyber security specialists. Based on this information thesis suggested 3 policy options which were tested against 5 criteria and have chosen the rational model as the most desirable policy route to improve the cyber security practices within the E-Government system in Azerbaijan.

Keywords: Azerbaijan, Cyber Security, E-Government, Action Plan, Rational Model

This thesis is written in English and is 77 pages long, including 6 chapters, 6 figures and 3 tables.

Annotatsioon

Küberturvalisuse olulisuse tõusust riigitöö teostamiseks, otsib Aserbaidžaani valitsus pärast e-riigi süsteemide rakendamist kõige sobivamat turvapoliitikat oma kodanike andmete turvalisuse tagamiseks vältides seejuures valitsusasutuste vahelise infovahetuse ohtu seadmist. Käesoleva magistritöö eesmärk on leida kriitilisi vigu valitsuse rakendatud küberturbe poliitikas ning anda hinnang parimatele võimalikele lahendustele. Magistritöö hõlmab eelkõige kvalitatiivseid uurimismeetodeid viies läbi juurpõhjuste analüüsi leitud probleemidele ning intervjuusid kahe küberkaitse spetsialistiga. Tuginedes eespool läbi viidud analüüsile annab käesolev lõputöö kolm soovitust valitsuse poliitika parandamiseks. Soovitused on testitud viie kriteeriumi vastu kasutades „Ratsionaalse mudeli“ teooriat mis tagab parima küberturbe poliitika rakendamise, et parandada küberkaitse praktikaid e-riigi süsteemides.

Märksõnad: Aserbaidžaan, Küberturvalisus, E-valitsus, Tegevuskava, Ratsionaalne Mudel

Lõputöö on kirjutatud Inglise keeles ning sisaldab teksti 77 leheküljel, 6 peatükki, 6 joonist, 3 tabelit.

List of abbreviations and terms

ANAS	Azerbaijani National Academy of Sciences
ASAN	Azerbaijani Service Assessment Network
B2G	Business-to-government
C2G	Citizen-to-government
C3	Communication, command-and-control
CERT	Computer Incident Response Team
CIA	Confidentiality, Integrity and Availability
CIS	Commonwealth of Independent States
DDoS	Distributed Denial-of-service
DoS	Denial-of-service
E-Government	Electronic Government
EaP	Eastern Partnership
EGDC	Electronic Government Development Centre
ESC	Electronic Security Centre
EU	European Union
FDI	Foreign Direct Investment
G-Cloud	Government Cloud
G2B	Government-to-business
G2C	Government-to-citizen
G2E	Government-to-employee
G2G	Government-to-government
GCI	Global Cybersecurity Index
GDP	Gross Domestic Product
ICS	Industrial control systems
ICT	Information and Communication Technologies

ID	Identification
IT	Information Technologies
ITU	International Telecommunication Union
MDCOC	Main Department for Combating Organized Crime
MIA	Ministry of Internal Affairs
MinCom	Ministry of Transport, Communications and High Technology
MRDA	Multi-Response Desirability Analysis
NATO	North Atlantic Treaty Organization
COVID-19	Coronavirus 2019
NCSI	National Cyber Security Index
NCSS	National Cyber Security Strategy
NGO	Non-governmental organizations
SAPSSI	State Agency for Public Service and Social Innovations
SCADA	Supervisory Control And Data Acquisition
SSPS	Special State Protection Service
SSS	State Security Service
SSSCIS	Special State Service on Communication and Information Security
UK	United Kingdom

Table of Contents

List of figures

List of tables

1 Introduction

Presently, cyber security is one of the crucial fields for the governments when it comes to ensuring the national security interests of any state. This happens due to the fact that most of the government data and information is now stored in certain databases. Moreover, with the rising number of cyber-crimes and the increased intensity of attacks to the states' cyber space, this problem grows into the issue of political importance. For instance, in order to increase their work effectiveness, the governments provide their civil services by using networks; and, such networks play an essential role in supplying the citizens of the country with the daily necessities like potable water, electricity, heating, natural gas and other pillars of energy. In this case, government rather uses the networked control systems to manage complex services, and such systems are commanded from the governmental software which later becomes subject to external attacks. This kind of situation politicizes the essence of using cyber security in the field of government. Therefore, the protection of those strategic data constitutes an essential pillar of national security. On a similar note, almost all of the government constituents and bodies share this common mission in several fields of their work and activities.

E-Government is one of such spheres where the application of the cyber security system is gradually being essentialized. E-Government is defined as the system of governance for providing the government services and information online and through computer networks (HarperCollins, 2018). It functions as a tool for "changing how governments work, share information and deliver services to external and internal clients" and it serves to gather "information and communications technology to transform relationships with citizens and businesses, and between arms of government" (Bhatnagar & Deane, 2004, p. 1). Such a system helps the governments not only to speed up their operations and services but also to effectively link separate state databases into a single scheme. The fact that e-government stores so much confidential and private information requires the establishment of a state-level mechanism for protecting their security.

1.1 Research Problem

Azerbaijan, as well as many other small states of the area called post-Soviets, have faced common challenges such as the necessity to build a new system for governance in a secure way after the collapse of the Soviet Union. The demise of the Soviet Union laid a foundation for Azerbaijan's relative backwardness in the preservation of its cyber space from the external aggressors. The problem of the gaps in the cybersecurity framework of Azerbaijan is potentially one of the most exigent issues threatening the top-notch confidential information stored in the state databases. Since Azerbaijan is currently applying a new, electronic system of governance into its state management structure, the problem with the prevention of attacks from external dangers are becoming ever more trending (Asan Imza, 2018). In this light, the thesis focuses on assessing the advantages and disadvantages of continuing with the current system for strengthening the cybersecurity of the E-Government in the country. The primary goal of the research study lies in evaluating the compatibility of the cybersecurity system applied in e-governance of Azerbaijan. The main aspect of study is its focus on the development of security strategy for the e-Government infrastructure in the country, that is ICT-powered use of government services, in Azerbaijan. In the second part of the study, the proposal of improvement action plan is provided that is intended to address existing policy problems and gaps which have been verified based on the selected success measures. Recognizing the importance of cyber interference from the side of the state, the thesis aims at analysing the current state policies for improving the defensive mechanisms practiced in the E-Government.

Azerbaijan has a real problem as it confronts the violation of its cyber-borders and penetration of destructive viruses into the state systems. It is crucial to stress out that Azerbaijan experiences such problems in the period of implementing very serious state projects. Azerbaijan's low ratings in the National Cyber Security Index as well as in Global Cyber Security Index gives us reasons to worry about these issues (ITU, 2018). Taking a historical lesson from the gap and vulnerability analysis of the current problem, this paper conducts a research study to analyze the reasons why Azerbaijan has been far behind in terms of advancing cyber security solutions to public governance and to propose an action plan which could assess the most desirable policy solutions in this light.

1.2 Research Questions

State computers and networks might get exposed to those policy gaps and existence of huge state formations as E-Government provokes the signs of warning for potential risks in the face of information losses. The foremost problem with the existence of response lagging in the system is that the consequences may directly inhibit the state's crucial services sphere. Consequently, such complication leaves the important information stored in the servers of E-Government vulnerable to attacks from outside sources. In the light of such operational shortcomings of local cyber security response teams, Azerbaijan ranks in the perfectly middle positions in the global database for measuring and reporting cyber security champions, National Cyber Security Index. Azerbaijan scores 37.66 out of 100 points while government authorities invest huge finances into the improvement of the sector’s competitiveness in the global arena (NCSI, 2020). Thesis further explores the reasons and factors bringing about such an outcome and address the following research questions:

Research Question #1: What are the causal factors and mechanisms affecting the deficiencies in the current cyber security policies within the E-Government of Azerbaijan?

By taking the account of the problem at hand, the research paper takes specific direction in favor of researching the opportunities provided by the new system for digital security. The ultimate goal of this E-Government system is to raise the level of security of domestically stored information. Estonia, one of Azerbaijan’s close partners in the sphere of cybersecurity collaborates with the local government to strengthen the foundations of a new model for electronic governance (e-governance) in Azerbaijan. Today, the government establishes institutions monitoring the level of cyber governance within the boundaries of cyberspace belonging to local governmental bodies. Such institutions and organizations specialized in information security play one of the crucial roles in designing plans and monitoring the rate of success assigned for the projects. These projects are mainly initiated for protecting the safety of cyberspace and are being a new problem-specific type of governmental formation. However, they still lack the experience to construct a mechanism for systematic response to external attacks and aggressor-powered assaults on the vulnerable layers of cyber security infrastructure in Azerbaijan.

Besides, newly gained independence of Azerbaijan is characterized by the lack of legal framework for conceding the provisions as to which practices in the sphere of cyber network are allowed and which norms are against the law. Unregulated nature of cyberspace of Azerbaijan had considerable negative impacts on the country's lagging behind the technological giants in this field. The security of the governmental data and information started getting more attention since the late 1990s when the legal frameworks on the protection of information became very important for the government as stated in the 1998 law on information (The National Assembly of the Republic of Azerbaijan, 1998). In this sense, the government further prioritized the issue of achieving such legal structure in its strategic roadmap (Ministry of Communications and High Technologies of the Republic of Azerbaijan, 2016) Legal basis for assigning a juridical meaning to the concept of cyber security as well as laws and regulations for determining its status and terms were the factors that contributed for the initiation of movement to introduce cyber security to the public in Azerbaijan.

As mentioned earlier, the thesis delves into solving the current policy challenges faced by the E-Government, which was established in 2012, and seeks to respond to those issues are also at the high stake and are under the watch of the authorities. Laws and regulations are accepted by many states involved in the practices of providing safety for the digital space of domestic information infrastructure. Thus, they are the primary determinants of the further dynamics and in the developments as well as deficiencies of informational structure of the domestic companies and agencies. Therefore, determination of the effects of the legal framework on the dynamics of improvement in the countries' cyber security credentials serves as research priorities and lay as the benchmark of assessment and evaluation of the policies conducted so far and proposals with regard to the new action plan for improvement in the information systems integrity for E-Government. Having said that, our thesis employs the following research question answers to which might provide as a solid alternative for the analysis of the possible policy directions:

Research Question #2: How can Azerbaijan improve cyber security infrastructure of the E-Government and which model should it pursue?

Thesis questions the compatibility of the policy models vis-a-vis the current Azerbaijani experience in the cyber security of E-Government. It looks through the possible ways in which the government could have made it possible to improve the existing state of the security in the cyber space of the governmental agencies operating through the system of e-governance. The main inputs for developing the action plan for the government comes from the interviews taken from the experts in the cyber security field as well as from the academic research. Through the information gained from them the thesis manages to analyze the data from the lenses of two separate state organizations for the fulfillment of comparative examination. On one hand, e-government theories employed in the model explain what are necessary elements that are needed to be included in the model for E-Government. On the other hand, the action plan based on the Multi-Response Desirability Analysis (MRDA) model exemplifies how those outputs are to be achieved. MRDA puts forward rational model, “garbage can” model and status-quo models as policy alternatives; and, it measures their susceptibility towards success through introducing measurement criteria. This technique allows the thesis to scale up the advantages and disadvantages of each method for public policy analysis and select the one more amenable for success.

Following these two research questions, the thesis tries to analyze the roots of cyber security challenges faced by E-Government, design and propose new policy directives for championing the solutions which have proved effective in the cases preceding Azerbaijani experience.

2 Methodology

Thesis, provides a deep insight into the research of the perspectives and resources available for improving the existing cyber-security framework. The paper especially elaborates the role of the efficient e-governance systems in the provision of state guarantee for the safety and protection of the computer systems and networks all over Azerbaijan. The research study involves the qualitative method of research analysis of the cyber security policies in the case study of Azerbaijan and elaborates its fit to the E-Government platform of the country.

2.1 Qualitative Methods for Study

The main challenge while conducting the study is the application of the most effective and efficient models. Such models are aimed at the development of the policies to provide a full safety package of the protection of the internal information of the country. This issue requires the analysis of the variables that affect the progress achieved by the state in the field of secure file transfer and storage which are not vulnerable against external attacks. Since the research seeks to determine the most influential factors affecting the emergence of the gaps within the cyber space of the country, the analysis of independent events is utilized in the procedure of data collection.

One of the main methods for analyzing the data in this thesis is policy and report analysis which is conducted alongside interviews. This method helps to examine the different policy events and independent evaluations of different authors about the mentioned research problem to help create a larger framework of ideas and structures out of patterns observed in the interviewees' speeches. Besides, the research study engages in the content analysis method of social research to analyze the data found in academic sources and artifacts. It comprises the study of state policies, statistics and composition of information out of the raw data. The official statistics published in the reliable sources are looked at from the critical viewpoint and data collection as well as measurement operations are being put on a rigorous analysis upon further contribution towards the gap analysis in the cyber security framework of Azerbaijan. Data collection also involves the application of online interviews with the experts of the field who are representing the institutions leading the country in the sphere of cyber security providing the protection against external cyber criminals, shields the essential data and information from being exposed to the hackers with malicious intents and fortifies the framework for better preparedness against any types of attacks from the unintended sources. The interviewees are cyber security specialists from Electronic Government Development Centre (EGDC) and State Agency for Public Service and Social Innovations (SAPPSI) who agreed to respond to the questions related to the cyber security initiatives as well as programs conducted in Azerbaijan. The purpose of the interviews is to gather the additional data for the Multi-Response Desirability Analysis (MRDA) for the identification of the policy route most desirable to the government and conducive for improvement in the cyber security of E-Government in Azerbaijan. Interviews are recorded through the mobile devices and are held in a passive format, distantly over the phone due to the limitations on free movement. The data analysis is performed through the transcription of the documented interview applying the clean verbatim style of communication recording, i.e. filtering of the text from the unnecessary filler words, incomplete sentences or vulgarisms used by the speaker employing the paraphrased wording.

2.2 Proposal of the New Action Plan

The paper introduces a new action plan for the government to implement on the way towards the advancement of the solutions to the cyber security challenges in the sphere of E-Government. The necessity for conducting new sets of reforms are important tools for addressing the challenges of the existing system. The focus and magnitude of the study directs towards the identification of the causal factors of the problem and the collection of the raw primary data which are upon contributing to the three distinct types of approaches to public policy making in the implementation of security-driven models. The first model is a rational model for applying a completely new and unique security system. It often proposes a country-specific solution to the problem and bases its decisions on the results conducted from the cost-benefit analysis of the underlying governmental projects (Einsiedel Jr., 1982). The second is called the “garbage can” model and it looks into the deepest historical records of the country’s past execution projects. The model tries to put the decisions of the past into the effect again through adapting them into the reality of modernity and redefining the timing of those plans. The main difference of such an approach towards public policymaking is its retrospectivity, state of choosing policies based on their application in the past (Cohen, March, & Olsen, 1972). The third model is status-quo, is an expectation of no change in neither the magnitude nor the quality of the current actions on the improvement of cybersecurity planning policies. Therefore, new effects are not foreseen during the process of such an approach's application, rather it aims at and ensures to protect the executive body in charge of the process from the possible wrongdoings and negative effects as well as costs of taking other approaches alternative to status-quo (Smith, 1979). These policy models are widely used in the sphere of public policy articulation and practice; and, discipliner scalability makes them applicable to the measurement and judgement of the policy routes discussed in the thesis.

Special emphasis is put on the solution part of the thesis where the consecutive implications inferred from the analysis of the current state policies that are devised for achieving specific accomplishments in terms of providing highly secured cyber space. Referring to the analysis of the cyberspace of the country through collecting the data from the existing institutions and organizations, the thesis proposed the improvement plan to incur positive impacts in the sphere of developing an advanced security for the cyberspace. One of the main priorities of the paper is to examine and provide an evaluation for the effectiveness of intergovernmental partnership between the states of Azerbaijan and Estonia in the integration of X-road implementation program which is being tested as an efficient and secure model of electronic governance. In this light, the thesis takes an interview from one of the experts representing EGDC and SAPPSI to discuss with him and get answers to the questions. The primary purpose of interview questions is to extract all the needed information on the policies pursued by the agency over the past years and plans for building up more capacity for the safe cyberspace in Azerbaijan in the future. Timeline policy analysis is one of the keystone tools we, as researchers, use for producing valid and reliable findings.

As such, the thesis undertakes the multi-response desirability approach towards finding out the most outcome maximizing result from the sets of policies being offered to enhance the cyber security framework in the functioning model of E-Government in Azerbaijan. It tests the policy options offered as a result of several research materials and data collected by the author. As such the new action plan for the government of Azerbaijan's recommended policy arrangements are suggested through the use of 5 criteria for the impact measurement and the selection of the most suitable strategy for it: those criteria are effectiveness, efficiency, feasibility, political viability, equity based on the policy alternative evaluation criteria used by the Michael Kraft and Scott Furlong's analysis models (Brajshori, 2017). These criteria help the thesis to measure the rate of success of the particular policy directions and serve as the basis for the indication of the empirically most durable project for the state administration.

The following, latest, subsection of the action plan concerns with the case of Georgia as a legitimate example for the investigation of the gaps of Azerbaijan which were followed during the policy making around the cyber security and e-government agenda. Sub-section defines and verifies the reasons for the similarities and mentions which problem it solves through conducting two case study country comparison. As a result, the effectiveness of the both policy routes applied in Azerbaijan and Georgia are critically examined to come out for a conclusion that resolves the existence of gaps in the decision-making procedure of Azerbaijani government.

3 Literature Review

The research projects specifically targeted at the examination of the data on ICT-related dynamics and its progress in Azerbaijan; unfortunately, such improvements were rarely accomplished, not to mention the fact that the cyber security area was inadequately studied. Nevertheless, due to both public and private sectors' exponentially growing interest in the field, cyber security came to the light and gained importance in a matter of recent years. This part of the thesis will, firstly, introduce the nature of the cyber security challenges faced by the government of Azerbaijan by explaining them through lenses of e-governance theories developed by the scholars in the field.

3.1 Theoretical Framework

The theoretical framework sub-section elaborates on both research questions addressed in the Introduction part. Initially, the first subsection will be presented, labelled "E-Governance Models – Solving Security Issues in Phases" to particularize the cyber security problems in E-Government of Azerbaijan. As such it will provide the background for finding answers to the 2nd research question to assess solutions for closing the security gaps in E-Government. It offers the concepts which would help to establish design for solving the underlying challenges arising from the implementation of the fully integrated E-Government system in the country.

Following, the paper proceeds with the sub-section which possesses the explanatory and predictive power of inter-state relations. Furthermore, it particularly analyses the outcomes of those which lead to the cyber security discombobulations to the domestic control systems of smaller states, such as Azerbaijan. Those theories will enable the reader to get the response to the first research question which aims at explaining the possible causal relationships in which Azerbaijan fails to guarantee the security of the citizenship data, pushing it to pursue a stronger E-Government model for stronger cyberspace and information security of the national data.

E-Government, as a relatively modern phenomenon, has existed since the late 20th century till today as the world saw the rise of information and communication technologies rise. Its primary function is to digitize the delivery of the governmental products and services to the citizens at home; and therefore, save time, energy and costs associated with the delivery of such services (Conklin & White, 2006). Azerbaijan, after the collapse of the Soviets, have started the implementation of the E-Government project since the beginning of the 2nd decade of the 21st century. The reason for such a response was inability to monitor the attacks from the foreign source as well as the inefficiency of the government apparatus (International Telecommunication Union, 2014). On this regard, it is crucial to understand the models of e-governance and to refer to the scholarly literature in order to track the implications of certain policies and to analyze the relative advantage of pursuing one policy route as opposed to another (implications for Azerbaijan are analyzed and applied in sub-section 4.2).

The main concept behind the application of E-Government is the underlying assumption that the model formed by confidentiality, integrity, and availability, also called CIA triad, is fundamentally taken seriously (Dhakal, Amatya, & Bal, 2012). Confidentiality is defined as definite rule and criteria determining who can access the information, integrity is about the trustworthiness as well as the consistency of the data, and availability involves the provision of assurance that authorized people are free to reliably access the information (Ada, Sharman, & Gupta, 2009). These principles are at the core of any security system and their application into Azerbaijani E-Government implies to take the advantage of the existing theories in this subject.

2 areas of CIA application implications in the context of E-Government implementation are the ideas of information security as well as cyber security (Molnar, Janssen, & Weerakkody, 2015). While many people use those phenomena interchangeably, there exists a systematic difference between the two, the former is concerned with the preservation of confidentiality, integrity and availability of the business/state information. However, the latter part is the larger concept of security as it comprises two layers. First layer is protection of data, especially what information security theory aims at doing. Moreover, the second layer is the defense of information and individuals placed in systems. It means that in case of E-Government, establishing a cyber security framework would not only mean to safeguard the information content, but also to safeguard the people who are within this network, including infrastructure and network

of the system. Nevertheless, new research studies on the issue suggest that cyber security is less about the protection and more concerned about the creation of resources that assist the institution to later employ them for better performance (Horne, Ahmad, & Maynard, 2016). Likewise, state uses cyber security framework in the process of applying E-Government into the state agency systems and networks to prevent harm to the people who work there, to the citizen data which can be tendered to the wrong hands, to the assets of state, to the systems which are in charge of controlling the strategic industrial systems of a country and so on. Therefore, implications of cyber security should be viewed from the broader scope, by seeing is not as a defense mechanism but the mechanism for stable work and many technical aspects of preserving stability while working with complex systems like the E-Government, will have to connect with cyber security issues (Schläpfer & Volkamer, 2012).

The implementation of E-Government as a state project is heavily dependent on the cyber security notions mentioned above. Therefore, when designing policies and strategies for constructing a reliable and secure system of e-governance one should be concerned with the right choice of modelling. In one of the studies on efficient and effective e-government modelling, research group proposed three pillars for the foundation of the system for e-governance: unique national identification mechanism to recognize the citizen data; method for citizens to legally relate themselves to any of the products and services provided in any government agency without compromising the confidentiality of a person; system or a platform which could not only store the data with utility but also to have multi-disciplinary approach for the satisfaction of the most varying needs, both for citizens and for state employees (Priisalu & Ottis, 2017).

While the above-mentioned research was conducted to lay out the fundamental theoretical base for the establishment of the system of e-governance, there are also research projects concerning the practicable aspects of E-Government which models its functionality based on the 4 stages. The 4-phase model of E-Government belongs to Layne and Lee (2001) who introduced four steps which would constitute a transformation from the basic towards the fully-functional electronic government. They devised a route for such transformation by identifying the stages necessary to pass starting from the presence stage for the realization of this goal. The first phase is the transition from presence to integration, the second phase involves the switch from integration to transaction, the third implicates the shift towards transformation and in the last phase, the system promotes openness and sustainability. 4-stage model of E-Government passes through sets of various procedures in the aftermath of which government starts by opening a web platform for its services and then gradually moves toward being more transparent through allowing for citizenship engagement and for the provision of all government services electronically with the highest level of security guaranteed.

Andersen and Henrisken (2006) have extended the model by proposing a new Maturity Model for E-Governance to express their own scope of the model. Their idea included the additional phase in which openness and eco-sustainability have the potential to transition to the co-production which implies that ICT will no longer be a problem for anybody; therefore, social innovations become the primary public service tool diffused across all the sectors relating to it. This type of new model has considered two main drivers of E-Government, such as citizen centricity based on people and organization; and process orientation based on technology and information. For the system to be upward-sloping, both drivers should be intact and co-exist mutually (Awoleye, Ojuloge, & Siyanbola, 2012). That system has some implications for Azerbaijani E-Government implementation projects, too. This is because it offers the vision relating to the outcomes of the ideally planned e-governance mechanisms; that is why, the system helps to find the crucial gaps existing within the domestic e-governance of Azerbaijan, effectively explaining where one may find the mistakes within the boundaries of policy cycle on E-Government. The progress on the status of E-Government with such a model becomes easier to track as there exists mechanisms for measuring success based on the increased citizen trust in the E-Government (Maric, 2014). The more people get involved in the process of service delivery through the electronic government platforms, the better governmental services become. With the methods for measuring success through specific indicators, governments own the chance to better integrate their services into the digital format and personalize them over many different types of people who are using their services (Savoldelli, Codagnone, & Misuraca, 2012).

3.2 Local Risk Factors and Possible Threats

As mentioned earlier, cyber security is ubiquitously expressed as the phenomenon that is slowly becoming one of the keystone priorities for national defense spheres.

Unfortunately, many small states, including Azerbaijan, had to start building their digital information structure from scratch as the centralized governance model of the USSR discontinued in the late 20th century. This situation was preceded by the unprecedented risks which were uncommon for the most part of the 20th century. Thereby, such small states happened to worry more than others as they underwent severe attacks and pressures by the giants of cyber warfare who are also technological leaders in their regions. In the case of Azerbaijan, it is even more complicated due to the fact that is being squeezed in between Russia, Iran, two of the cyber powers of the region and Armenia, the potential threat for the national cyberspace. Therefore, starting from the recent years, Azerbaijan commenced to pursue policies for strengthening the internal protection and building up partnerships with countries such as Estonia in order to learn from the past failures as well as present achievements gained by the employment of the e-governance model of the local government (Asan Imza, 2018).

Not long ago, Sandworm Team based in Russia was a threatening actor in the cyber warfare against many post-Soviet states like Georgia and Ukraine. Their attacks carried the purpose of committing DoS attacks through targeting the victim's domestic networked control systems such as the electrical utilities, transport control systems, financial and manufacturing industries which all operate thanks to the integration of the computer networks (Morgus, Fonseca, Green, & Crowther, 2019). Azerbaijan underwent two cyber-attacks similar in nature with that of Sandworm Team's critical infrastructure DoS attacks during the period of 2008 to 2012, the former being the year when Baku-Tbilisi-Ceyhan, the main pipeline which serves country's most of the exporting capacity; the latter being the year when the MinCom, the Ministry of Internal Affairs and the Ministry of Education and other government organizations as well as media websites were massively hacked (Panahov, 2016). Sandworms are also known of being attributed to the Main Centre for Special Technologies of the Russian General Staff Main Intelligence Directorate which operate under many secretly coded names from BlackEnergy Group to VoodooBear (Roguski, 2020). Specialists from the UK have conducted a comprehensive analysis of their actions which revealed that the attack to Georgia was almost certainly coming from the cyber adversaries which are called "Sandworm"s (Foreign & Commonwealth Office; National Cyber Security Centre; The Rt Hon Dominic Raab MP, 2020).

It must be pointed out that the both incidents, especially 2012 attack alarmed the security bells of number of Azerbaijan serving as the indications that the country needs to improve its digital infrastructure to catch up with the technological speed prevalent in the world. As thus, Azerbaijan has already tightened its regulations and started demonstrating rather stricter stance towards building up an information ecosystem and networks which are reliably secured by the strengthened network incidence response mechanisms created as a result of the established national policies and legal frameworks which allowed for progress in the mentioned sphere. One such policy is related to the protection of the state secret and confidential information which the state databases are organized upon. On the 10th of February 2014, the President of the Republic of Azerbaijan Ilham Aliyev decreed the approval of the "State Program of the Republic of Azerbaijan on development of the protection of the state secret for years of 2014-2018" the administration of which former Ministry of National Security of the Republic of Azerbaijan (current SSS) was in charge of (Cabinet of Ministers of the Republic of Azerbaijan, 2014).

3.3 Domestic Policy and Legal Basis

Thus, as a state that has already undergone cyber-crimes, Azerbaijan plans to counterbalance violent actions of hidden rivals in the cyberspace. Consequently, cyber-security is ranked as an utmost issue in the policy of Azerbaijani officials (Respublika, 2019). Intercontinentally, Azerbaijan Republic is a solid protagonist of cyber laws and is implementing preventive laws of illegal activities against the committers of cyber-crime). Its first law regarding this matter was issued in 1998, when the parliament adopted *Law on Information, Informatization and Protection of Information* which was granting the security of any outcome of creative works secured by universal intellectual property rights such as patent, copyrights, trademarks and that also served as the basis for the law on the protection of the data of the state secret.

The CoE appreciated the movement promoting cyber laws in Azerbaijan on June 30, 2008, when it joined the Convention on Cybercrime. Subsequently, computer experts of Azerbaijan were triggered to combat cybercrimes and other illegal actions (Makili-Aliyev & Attiq-ur-Rehman, 2013). Thus, Azerbaijan was one of the active members of the world's first pact banning unethical and immoral usage of internet and cyberspace). Konstantin Yerokostopulos, the former head of Council of Europe highly appreciated the Azerbaijan's support to the fight against cyber-crimes in the Budapest Convention on Cyber Crimes. The essential goal of the Budapest pact contained the misuse of the computer networks, "infringements of copyright, computer-related fraud, child pornography and violations of network security".

Together with above mentioned many-sided activities, Azerbaijan is designing its own laws for prevention from internal cyber-crimes. Ilham Aliyev, the President of Azerbaijan, has signed a decree to upgrade the cyber-security situation in the state. The safety and security of electronic resources of Azerbaijan government are mainly concentrated in this decree (Mission of the Republic of Azerbaijan to NATO). Rendering this decree, under the supervision of MinCom there is established a centre of coordination structure for electronic security. The cyber-legislation is divided into two parts: prohibition of computer abuses and strengthening of cyber-security. One is "Law on National Security (June 2004) and other is the Law on the Protection of Unsanctioned Information Collection (September 2004)." Besides, the Azerbaijan Criminal Code defines in its Chapter 30 (titled: Crimes in the Sphere of Computer Information) computer resources that contain such areas as "unauthorized access to, and breaches of the security of computer systems, including the development and use of computer virus" and rules and regulations on internet. The penalties in the forms of fines and imprisonments are defined for the security of information communication networks and for the stoppage of internet abuse. Actually, law of National Security of Azerbaijan has passed in order to stop local trespassers, but the real danger comes from external cyber criminals conducting illegal procedures. Efficient and proper cyber laws are needed to be introduced in order to prevent malicious activities in the virtual reality. According to A.R.Panahov, measures taken by the Azerbaijan government against the cyber-attacks, internet crimes and malpractices of information communication networks, political cyber action is still used as a political tool to manipulate the victims of the cyber-attacks and thus, highly probable threat to cyber-borders of Azerbaijan (Panahov, 2016). The government should eliminate malicious actions and respond to them adequately. The government authorities responsible for security of digital control systems should strengthen the protection of computer networks and add reforms to existing laws while revealing new areas to defend and evolve national cyberspace. One of the recent examples showcasing the state attention toward information security is the whole new legal project on the protection of private information. The Law on Private Information" that came into force starting of 11 May 2010. The function of this legal act is described as defining the principles of state regulations on the establishment of information systems and information sharing, as well as to protect the confidential data and information of the citizens of Azerbaijan (National Assembly of the Republic of Azerbaijan, 2010). The law introduces primary terms for the licensing of the information systems, as well as accounting for the confidentiality rights of the subject (the one whose private information is collected) and liabilities of the enterprises and system operators by specifying the legal limits of their utilization of private information. It also lays out all different forms of state regulatory practices and showcases the different categories of the private information. Overall, as a new-born phenomenon, legal understanding of the information security in Azerbaijan can be referred to as the foundation of the country's cyberspace protection policies.

The legal basis of cyber-security needs to be strengthened in Azerbaijan because, the cyber-weapons in different forms (such as an attack conducted by the Sandworm Team) have already attempted to destroy the government cyber-infrastructure throughout the post-Soviet countries for political reasons. So, a strong and well secured cyber-network can prevent the risks of cyber-attacks in the digital infrastructure of the country. Furthermore, the promotion and advancement of cyber laws with the establishment of a cyber-army has become a vital demand for Azerbaijan in order to strengthen the national cyber-security of the state (Xeberler, 2014). In this way, the safety and security of cyberspace is a matter of mammoth significance for Azerbaijan, because the growing dependence of industry, government and financial institutions on cyber-networks needs a completely secured and reliable information system, which could maintain cyber-deterrence in the global cyberspace. As of today, Azerbaijan has not revised its educational goals and reforms aimed at improving the cadre preparedness in cases of cyber-adversary attacks and thus, the higher education system offered no officially certified and approved courses on cyber security till 2018 (Asadli, 2018). Currently, there is only one institution that trains and instructs future specialists on cyber security, Baku Higher Oil School (Zulfigar, 2020). Nevertheless, one of the recent improvements on this path is the decision of the former Minister of Education of the Republic of Azerbaijan, Jeyhun Bayramov, on the establishment of the Board of Trustees consisting of 18 members for the revision of the list of specializations in high educational institutions of Azerbaijan (Ministry of the Education of the Republic of Azerbaijan, 2020). The current Chair of the Board, the vice rector of ADA University Fariz Ismailzade has mentioned that the Board has decided upon introducing cyber security, along with many other technical subjects, as a mandatory course for the students at the university level (Ismailzade, 2020).

Even though Azerbaijan's national cyber security strategy is yet under the process approval, the fact that it has been already completed and presented upon further revision tells that the domestic cyber security policies in the country are newly becoming popular among the public as well as the private sectors (Azertag, 2019). As of 2011, Azerbaijan has made it to the leading positions in the ICT sector in the region of CIS as it started investing in policies which led to the development of the ICT field within the country (ITU, 2018). 2013 year was announced to be the year of ICT and people as well as the organizations all along the country were incentivized to produce innovative ideas as well as the products and services since an extensive support from the government was offered in return (Cabinet of Ministers of the Republic of Azerbaijan, 2013). This type of incentive was one of many series of events which truly dedicated a lot of attention to the influence and prosperity which Azerbaijan could gain as a result of developing its proficiency in the sphere of information technologies. Among other facts, the need for the national policies and the stance of the government on the status and importance of carrying out reforms and improvements in the information security field is explicitly reflected in the "National Strategy of the Republic of Azerbaijan on the Development of the Information Society for the years 2014-2020" (Cabinet of Ministers of the Republic of Azerbaijan, 2014). The fact that the word "cyber security" is mentioned only 5 times, less than the word information security which is used 15 times, delivers the message about the relative prioritization of one specific aspect of cyber security rather than a comprehensive strategy and guidelines for the executive branches of the government on building up cyber security framework for the country networks. Instead, the article 10 is dedicated to the development of the fully functional e-government while the article 13.2.4 instructed the provision of information security for the e-government infrastructure (Cabinet of Ministers of the Republic of Azerbaijan, 2014). The main governmental body responsible for conducting such initiatives in the sphere of information security is MinCom of Azerbaijan. MinCom is responsible for operating the largest data storage centre in the South Caucasus, called "AZCLOUD" Data Centre as of December 2016. The mentioned data centre is the first place in Azerbaijan and the region to fulfil the data security management standards and receive an official recognition as the TIER III, ISO27001, ISO22301 and ISO20000 certified institution (AZCLOUD, 2020). It possesses large capacity to reliably store and protect the data with the attachment to confidential state information. Apart from it, the ministry engages in work on the improvement of public response measures regarding the cyber security capacity building is mostly conducted through cooperating with the Eastern Partnership initiative launched by the EU and Azerbaijani MinCom is among the main stakeholders of "EU4Digital" project aimed at strengthening the integration of modern information technologies in the partner countries (Ictimaixeber, 2019). "EU4Digital" project is the one of the sponsors of innovative information security solutions applied by Azerbaijan in the recent years. Rashad Azizov, the Head of the Department of Innovative Development of Information Society and Electronic Governance of the MinCom, mentioned in his interview to that Azerbaijan currently finds himself in high-risk cyber intervention environment and that risks of information theft is on the rise as CERT of the SSSCIS reported an increase from 895 to 1200 cases, 34.1% spike, in the number of computer security requests by agencies relative to the January-April 2018 (EUFORDIGITAL, 2019). Presidential decree of 3 June 2019 is one of the main initiators of the most recent cyber security policy prepared by the government apparatus. It orders the establishment of the Government Cloud (G-cloud) for the purpose of cutting costs in public management and the improvement of the coordination among the state institutions. The underlying cloud technology will serve as the single centralized platform for the effective formation, storage, safe transfer and integration of the state information systems and resources (Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan, 2019). The state project implies the assignment of the platform into the authorization of the MinCom which will control and regulate the safe and smooth work of the system through the above-mentioned Data Centre which will serve as the primary infrastructure for storing the data that such platform is expected to store.

4 Cyber Security Policies in Azerbaijan

Today, the government of Azerbaijan works towards improving and reforming its ICT sector by making it more competitive in the global scale. This idea is especially required for its application on the implementation of E-Government projects (more detailed in the 4.2). As since there are many factors which challenge the safety of the cyber security framework in the countries with newly-established digital structures, availability of state support and control of the issues related to the protection of the cyber-borders of a country can be considered a vital issue. The alliance of significant structures of state like military, governmental issues, economy and social frameworks are heavily relying upon network systems. In future, it is probable that the politically charged allegations from the cyber-adversaries from external sources can violate the safety and security of the networked control systems as well as the government information (Makili-Aliyev & Attiq-ur-Rehman, 2013). Systematically, there are three reasons which rank Azerbaijan among the top vulnerable countries to the digital security dangers. First of all, there is a risk associated with applying interconnected networks within both public and also private sectors in the country. This implies that new cyber security challenges put under threat not only the government's own infrastructure, but also those owned by other entities like businesses, banks, or NGOs. Secondly, the growing tendency of internet users in Azerbaijan in the context of expanding information age tends to increase the interactions of Azerbaijani users with those of global network clients. This one especially leaves citizen data and information vulnerable to the external threats since the accessibility of the information grows easier. Ordinary internet users surfing across the web may have difficulty identifying safer sites for their experience and expose their confidential information to the existential risk. Since, the governmental services undertake to protect the confidential information about the citizens, the government provides safety measures by initiating systems like E-Government to reliably store such information away from getting exposed by external aggressors. In this light, cyber security of not only the E-Government but the whole cyber territory of Azerbaijan becomes an important cyber security challenge. Thirdly, the expansion of opportunities on the global networks makes spots such as the internet a conducive playground for a flourishing number of self-navigating as well as politically guided cyber-adversaries (Farajova, 2019). This in itself poses threats to the countries with underdeveloped or unprotected digital structures. Since Azerbaijan is relatively new to the business of developing the security infrastructure of its E-Government, cyber safety issues within this system have to be analysed thoroughly. The hostilities out in the virtual space may also threaten the legitimacy of the government of Azerbaijan, in case there are crucial failures of services. In such a situation, Azerbaijan finds itself in the digital environment that is highly exposed to the external dangers such as the cyber-attacks towards its strategic units. To put it plainly, cyber security challenges, following the worldwide patterns, are consistently getting the status of a significant worry for the government of Azerbaijan (Alizadə & Aliyev, 2018).

4.1 Cyber Security in Azerbaijan: Overview

The President of the Republic of Azerbaijan Ilham Aliyev has given an interview to the representatives of the media during the BakuTel-2012 event, the largest IT exhibition in the Caspian region, where he emphasized the serious nature of the challenges associated with the extension of the country's cyberspace (Bakutel, 2012). President Aliyev said that web security is turning into an essential issue. The dangers posed by the criminals, terroristic groups and organizations as well as the black-hat hackers made the national cyberspace a place susceptible to the foreign attacks, which will bring about cyber-warfare after the modern conflicts caused by the religious, natural resource and regional disputes (İmamverdiyev, 2013). In this light, cyber-crimes have become the subjects of state worry for their risk-posing nature accelerated as a result of an Internet becoming a necessary state tool for multiple purposes of the statecraft. That concern makes the construction of a protected and secured cyberspace a principal goal and political interest of a state. (Verdiyev, 2018).

Digital security isn't constrained to financial and social sectors of a state. It is also increasingly applicable to the military domain. The new information age gives an opportunity for the external adversaries' access of the critical infrastructure which means this type of development takes the idea of comprehensive application of cyber security measures not only limited to the citizen but to the new strategic level. In absence of such measures the country's military intelligence devices such as the censor (radar) systems, systems of communication, command-and-control (C3) as well as advanced computers regulating the technological infrastructure of the country would be victimized by the external aggressors. The main role of focusing on the military arranged networks of any state is just to defuse the opponent's capacities of focusing on, following and connecting with the hostile assaulting powers. Currently, developing virtual military capacities presented another type of military art which is commonly called an information war or warfare (Pawlak, 2018). The combat zone of information war has included the national governments, non-administrative associations, social networks, and corporate areas. Supplied with the power of digital advantage over some of the targets, cyber-adversaries perform attacks on the systems with little amount of data security and highly vulnerable data infrastructure which alarms those with similar levels of safety.

The information warfare has changed the traditional ways of organizing one’s defense mechanisms. New technologies which are actively used in the process information extraction and data leak lead to the new waves of concerns about the modernization of one’s virtual defense system; thus, the creation of nanotechnology and its application in present day digital warfare additionally creates the situation where even states and governments all around the globe become insecure as a result of lacking the capacity managing cyber attacks (Janczewski & Caelli, 2016). The attacks on the critical infrastructure of the states are the nice examples why the countries like Azerbaijan or its neighbor Georgia have become more worried about encountering the potential intervention. While 10 years ago the number of described incidents was very limited and the application of cyber security in the state policymaking was not an urgent task, same words cannot be told about today since Azerbaijan is modernizing its technological capacity day-by day and much more infrastructure is built that makes it prone to those attacks (Mammadov, 2008). The real-world signal that indeed made Azerbaijan worried was the realization of the security risks posed by cyber criminals (for example, when it was demonstrated by Sandworm Team attacks) which can lead to the digital assault having an undeniable effect in the physical world (BBC, 2013). All states, including Azerbaijan, are distinctly aware that systems and methods of information warfare are difficult to capture and deal with. While such attempts to disrupt the state network systems happened in the many post-Soviet states, including its neighbor, Georgia, Azerbaijan finds itself in an identical situation over the conflict with another neighbor, which forces the government of Azerbaijan to strengthen its cyber-resilience (Hasanli, 2015).

The likelihood of information warfare has encompassed the customary security instruments of regional sovereign states. Fundamentally, the ability to convince individuals is a potential weapon in information warfare, in light of the idea that the data age has increased the necessity of getting information, and the manipulation and abuse of facts can quickly undermine the social opinion on the nature of real facts and mislead the international community. At the end of the day, dangers of information warfare confirmed the status of the Internet as a progressively intricate and universal device for the warfare. The procedures of information warfare most likely will target the defense mechanism of the states. In such a rivalry, Azerbaijan may confront genuine risks of attacks since usually information warfare involves the weapons which attack the C3 systems to disrupt the transfer of crucial information between the intelligence services and state departments (Burton, 2013). The odds of mental tasks against Azerbaijani initiative, populace and social and national qualities may introduce a test to the security foundation of Azerbaijan in future. In this manner, the uncontrolled and unchecked development of digitization may turn into a significant risk for Azerbaijan, in light of the fact that a large portion of the people and associations which are relying upon the web are uninformed and unaware of standard security procedures needed to follow while using the internet; that is the essential motivation behind the primary open public project conducted by MinCom, “Cyber security week”, that operates on an annual basis starting from 2019 and leads discussions about the user responsibility on the online platforms, data security etc. with the presentations of the representatives of the world-leading tech companies such as the Microsoft (ABC, 2019). The circumstance may turn out to be increasingly genuine where the unconscious and ineffectively prepared web clients are ignorant about their helpless and exposed status. The suspicious online exercises generally allude to the eventual fate of the web, which could be envisioned as digital fear-based oppression. The non-state actors will turn into a gravest danger to the state to the extent that they accomplish the digital refinement (Conklin & White, 2006). In general, the analysis of cyber-attacks registered in the country shows that 90% of attacks are carried out from abroad and the sstatistics demonstrate that the intensity and number of attacks on the country's information resources is growing by 30% every year as small scale but frequent attacks have been confirmed by the European Union (EU) to incur huge economic and legal costs (European Parliament, 2017). The analyses show that some of the hacker attacks are motivated by political and economic motives. The analysis of attacks on Internet information resources by government groups, belongs to various government organizations, many of which organize their security through a group of hackers calling themselves "Anonymous" (CERT Azerbaijan, 2020).

4.1.1 State Institutions for Providing Cyber Security

Along these lines, the digital fear-based oppression can turn into a component of worry for Azerbaijan in future since the probability of digital fear-based oppression may arise against the residents or government due to the international conflicts which it finds itself in. To address the potential dangers in the internet, Azerbaijan is building up its own establishments that manage digital security. In order to act in an organized manner against possible cyber-attacks, there is a need for serious investigations of the incidents in the field of computer and Internet security, and for that reason the government in Azerbaijan have operationalized various institutions and agencies to lead the fight and response to such attacks. Those are the teams formed from the collaborative initiatives and based in the agencies such as Electronic Security Centre (ESC) under the Ministry of Communications and High Technologies, the State Agency for Special Communications and Information Security of the Special State Protection Service, the National Academy of Sciences and the Ministry of Education (Aliyeva, 2015). Those special groups consist of the best specialists in this field — Computer Emergency Response Team (CERT) under the Ministry of Communications and High Technologies of the Republic of Azerbaijan deals with the coordination of the activities of other information infrastructure entities operating in Azerbaijan under the CERT label.

Even though there is some involvemet from the public and private sectors regarding the provision of cyber-awareness and security of infotmation, the government mostly relies on its own administrative capacity and international cooperation with many security organizations. State provides digital security by the contribution of three principle bodies – Special State Service on Communication and Information Security (former Special Communication and Information Security State Agency under the Special State Protection Service), Ministry of Transport, Communications and High Technologies (Mincom) and State Security Service (E-Governance Academy, 2018). SSPS was a paramilitary legislative organization designed to protect critical state bodies and assets until the Presidential Decree on “Improvement of the management in the sphere of special state protection" of 16 March 2020 when it was dissolved into 3 main structures, one of which is SSSCIS (Qafqazinfo, 2020). Its command as of late additionally incorporates the digital security of state basic computerized systems and infrastructure. SSSCIS keeps up its own CERT and huge aptitude with regards to the defense of communications, alongside with the latest technology and equipment that permits it to cover a huge cluster of governmental systems. As of late MinCom has built up an Electronic Security Center (ESC), a body that is charged with the digital security of private networks and also is the center of investigating and analysis of many different cyber security issues. This system is also responsible for coordination part of the cyber governance of Azerbaijan as it informs and operatively works with the other state bodies dealing with many crimes based on the cyber-oppression (Yoon, 2019). Fundamentally, ESC is a mix of CERT for private systems and a information processing center for digital security. Simultaneously, the SSS also possesses sufficiently valid mandate to cover the digital protection of the state. Despite the fact that the main functions and responsibility over the most of the responses and enforcements over the cyber-defense issues fall heavily on the MinCom, SSS uses its mandate to intervene when the cyber security issues in question are coded as cyber-crimes and cyber threats such as in the case when commercial banks of the country were robbed by the foreign cybercriminals who ceased more than 3 million manats while compromising the information systems of those banks (Department of Public Relations of State Security Service , 2017)

As it tends to be seen from above, Azerbaijan keeps up a triangular arrangement of digital security organizations that have assumed their own proper position in protecting the digital security of the nation. The viability of the framework is the immediate nexus to the exhaustive digital safeguard of the state. Subsequently, such a framework will consistently require excessive levels of interagency coordination. It ought to be called attention to the idea that the internet has already been transformed from a ICT device to a fundamental component of world legislative issues, and it is prone to lots of potential abuses and misuses which can cause or even accelerate the domestic as well as the international political crises. The misuse of disputable qualities and control of data will scrutinize the current standards and guidelines of the internet in Azerbaijan. Universally, definitive unfriendly digital assaults will be the contending properties of world governmental issues. The mix of digital and information warfare will make all the states similarly helpless on the internet. The triumph of unfriendly powers by utilizing the virtual devices will challenge the sovereign state values. Because of such conceivable future outcomes, the computerized enactment ought to be improved corresponding to the digital security organizations in Azerbaijan.

4.1.2 Reasons for Slow Improvement

Despite the governmental efforts aimed at the improvement of the overall security provision in the network of the computers and electronic data servers, it does not manifest itself in the shape of the immediate outcomes. Instead, Azerbaijan takes very low scores on cyber security stats according to the different indexes such as National Cyber Security Index (NCSI) and Global Cybersecurity Index (GCI) where Azerbaijan barely gets into the first 100 among the world countries (NCSI, 2020; E-Governance Academy, n.d.). Many questions then arise as to why the country is experiencing such problems with having so low performance and the problems express themselves in both direct and indirect factors which are the driving forces behind the small-scale growth of Azerbaijan in the cyber security rankings. Content analysis of the literature on the legislation concerning cyber security as well as the policies conducted in this sphere were mostly incomplete or ignorant of the existing state of affairs. As it is observed, the government of Azerbaijan did not enjoy much of the determination in terms of putting the big efforts for improving its cyber security framework because it was not having the problems with attacks on an intensive scale. However, the sudden change in the direction of the policymaking on building E-Government and improving its security framework from close to nothing toward building sets of comprehensive systems can be explained through the realist theory. While the main talk goes on the establishment of E-Government as a state project, the government needs to ensure that no foreign power would be capable enough to access the strategic information it stores using such systems.

The main finding of the thesis was that the relative cyber-backwardness of Azerbaijan in this sphere should be observed in terms of two radically different periods of its investment strategies in the cyber security infrastructure improvement. This period is the time between the restoration of Azerbaijan’s independence till the beginning of the second decade of the 21st century, in other words between 1991-2010 and the period of 2011-2020. Relying on the nature and intensity of the policies and legal reforms dedicated to the technological transformation of the country infrastructure, thesis views the year 2010 the point of change in governmental attitude towards cyber security reformation. The reasons for such sub normality prevailing in the first interval should be traced back to the structural factors which affected the other important variables creating the domino effect. So, the main omission of the government during the years of independence was the late political will of the government aimed at changing the situation. Therefore, one must, firstly, admit that the main comprehensive policy of Azerbaijan for the formation of cyber response teams was the absence of such policies and this was reflected on many spheres. For example, the government of Azerbaijan has started the development of common national strategy for combating cyber-crimes only as recently as late 2019 (Ministry of Transport, Communications and High Technology of the Republic of Azerbaijan, 2016). This step is a very important pillar on the way of achieving excellent cyber-defence which can be seen from the fact that many advanced nations follow the same path. The main targets of adopting such a strategy would be the establishment of a cyber security framework controlled through the central system, elimination of legal enforcement gaps on the issues of cyber security which were not consistently implemented in the period before 2010s. This study revealed that Azerbaijani authorities have failed to provide timely response to the gaps in the cyberspace policies and that was reflected on the overall results, causing the structural factors which prevented the smooth functioning of the cyber security network in the country. Among those factors were the lack of the government willingness to carry out reforms in the digital sphere, absence of national cyber security strategy which would outline the cyber security framework in the central system, lack of legal framework on the issues of cyber security and its implementation terms until 2010s. There was the role played by the indirect factors such as the lack of strong cyber security and ICT education, small amount of domestic investments as well as the FDI in the mentioned field, high costs of infrastructure development and so on (Asadli, 2018).

As we may clearly observe from the graphs on state budget, the government investments on this field have been on dramatic rise since 2011 and recent years demonstrate that political willingness from the side of the government was indeed a main reason for the slow progress. Because the country was earning more during 2006-2010 than now, while it has been investing more since recent years. Figure 1. and Figure 2. demonstrates the patterns behind the rising fund allocations in this direction

(Chamber of Accounts of the Republic of Azerbaijan, 2017; Chamber of Accounts of the Republic of Azerbaijan, 2018; Chamber of Accounts of the Republic of Azerbaijan, 2019).

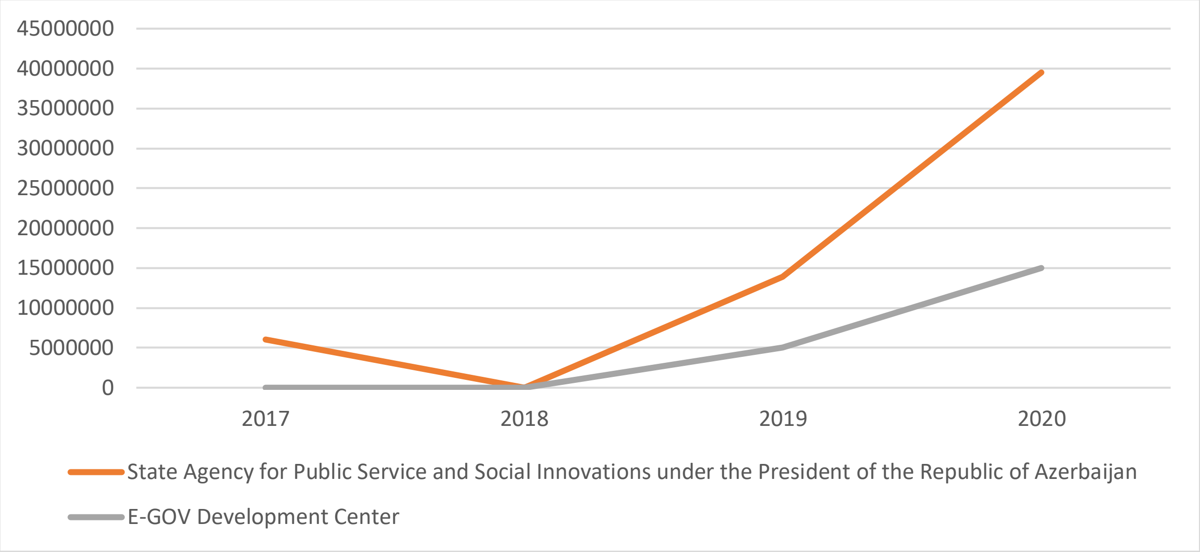


Figure 1. State Budget allocated on EGDC and SAPSSI in 2017-2020 (Statistical Committee of the Republic of Azerbaijan, 2020)

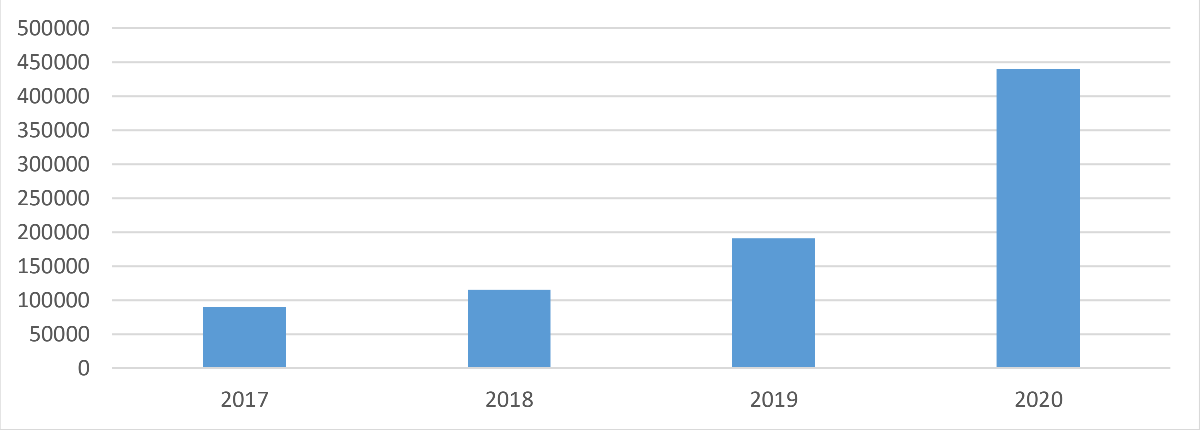


Figure 2. State Budget allocated on Computer Emergency Response Team under the MinCom 2017-2019 (Statistical Committee of the Republic of Azerbaijan, 2020)

4.2 Perspectives for E-Governance in Azerbaijan

All in all, cyber security is a very sensitive topic when it comes to the issue of state interests and its importance has been highly bolstered in every sector of government service since the 21st century's beginning. One of the key priorities of the government in Azerbaijan, today, is to ensure the safety of one of the specific types of sectors where government services are already in dense usage, that is the e-government (Adliyya, 2013). In Azerbaijan, interactive government models have turned into the prodigy for the government to facilitate the fulfilment of its services in a faster and reliable way. As such, e-government is the use of information and communication technologies for directly utilizing governmental bills and it is used to the communication channels between governmental agencies (G2G), businesses and the government (B2G), residents with government (C2G and G2C) and between the government and its employees (G2E).

It comes as no surprise that the state authorities and officials have started investing heavily in the development of nation’s digital framework for securing its cyberspace and every year it plans to level up national awareness as well as preparedness for cyber-accidents. One of the main state models which Azerbaijan follows and seeks for establishing mutually beneficial agreements with is the government of Estonia, and countries of North Atlantic Treaty Organization (NATO) overall as they have years of expertise in the localization of the threats posed by the external threats (Herzog, 2017). Therefore, the future investments in the sector of cyber security is expected to grow, through direct support by the government, in Azerbaijan in the following years. X-Road, prototype of which is already under the use in E-Government which uses the innovation to protect the security in the forms of digital signature, digital footprints and stamps; is a successful example of Azerbaijani-Estonian collaboration in the field providing protection for cyberspace (Asan Imza, 2018). Even though Azerbaijan does not own a long year of records for achievements in the mentioned sphere, there are already several positive outcomes. One of the primary examples showcasing the successful model and direction of the cyber security initiatives implemented within the prototyping of the X-Road initiative quintessential for the cyberinfrastructure of Estonia, is that Azerbaijan had successful cases with various state-level partnership and training offers for the integration and exchange of data mobility with the partner states such as the one addressed by Afghanistan. The statement which came from Deputy Minister of Information and Communication Technologies of Afghanistan Mohammad Hadi Hedayati mentioned Afghanistan’s strong willingness to exchange information with Azerbaijan in the field of cyber security and e-government. According to him, Azerbaijan has a good experience in the field of e-government and the country is interested in benefiting from the opportunities which strong collaboration can give them: "I think that Afghanistan can benefit from Azerbaijan's experience in the field of e-government" (ASAN Radio, 2019).

In general, the introduction of electronic services for the purposes of transferring government services to the digital format have been applied in Azerbaijan since 2012 when the President Ilham Aliyev signed a decree on the establishment of a new state body called SAPSSI (State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan , 2012). Its main product was the presentation of services in a transparent and partly digitized way delivered through the various different service points called Azerbaijan Service Assessment Network, or simply “ASAN” Service (Alguliyev, Yusifov, & Gurbanli, 2018). The idea was to facilitate as well as to centralize the procedure of providing essential state services such as the preparation of the passports, national identity (ID) cards, paying the communal fees, traffic bills, business registration fees and so on. Apart from it, a new electronic portal was also handed out for the public use by the citizens and businesses which made “ASAN” Service a popular and in-demand high-tech brand used by millions of people (State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan, 2020). This type of e-governance tool employed in the domestic policy making by the state administration have happened to increase Azerbaijan’s overall capacity for developing its E-Government systems since the new digital experience process with delivering fundamental state services gave the authorities an idea that the public here is indeed interested in the application of comprehensive and centralized platform to use such systems. The same principles used to lay the foundation of “ASAN" Service, was later applied to connect all state organizations into a single system for them to securely send each other data files, exchange and transfer information needed for the operational and efficient work. Azerbaijan’s initial success in the sphere of delivering the state services in faster, efficient and flexible ways improved its potential for transitioning smoothly to the E-Government by incorporating the most of the governmental data and information into the common system based on inter-state organizational exchange which is directly connected to the third party—end users. Since the E-Government comprises G2G, G2B, G2C, C2G, G2E connections in the business model of e-commerce, the scope of the impact it can deliver stretches to the millions of citizens, hundreds of state agencies and organizations and tens of thousands of private institutions as well as private businesses which all may utilize the state services which are screened to the end users as a result of complex security procedures as the state agencies enter new information into the common database. These policies can also prove the necessity for the application of the CIA and e-governance theories in practice. As such the government of Azerbaijan has been pursuing the set of comprehensive policies directed to enhance the cyber security framework in E-Government and has used its finances to prevent harm to its resources. Those resources included the people who were employed in those state agencies, citizens whose crucial data was stored in the systems, industrial control systems which are responsible for delivering communal services to the population and so on. In all these cases, the cyber security framework of the country played a crucial role for motivating the state to pursue policies that secure its people, organizations, networks and especially information. Azerbaijan is now in the transitioning process, as it has already switched to the 3rd, transactional, stage of Lee and Layne's models (Layne & Lee, 2001). Some of the state institutions and agencies are still incapable of integrating to the E-Government system of Azerbaijan. This means that even though there is a huge portion of citizen centricity, citizen engagement and popularity of using such systems, the process orientation driver (technology and information-based) of the procedure is improving less in speed than that of citizen centricity levels. This should serve as the starting point for the government to work on the improvement of, for achieving the fully integrated E-Government model as laid out by Andersen and Henrisken (Andersen & Henrisken, 2006).

4.3 Data Collection

In this section of the research study the author conducts an independent analysis of the findings which he gathered throughout the interviews with two experts in the field of the protection of the essential data and information stored within the state institutions' computer networks and digital systems. This section will involve the description and analysis of the communicated information about the subject matter. Interviews were recorded using the mobile phone sound recording feature and the recordings were manually transcribed into the document for enabling clearer analysis. Clean verbatim style of transcription was intentionally employed to avoid the capture of every utterance of the interviewees and instead to allow for focusing on what was being said in the manner which the subjects of the interview preferred to pronounce their ideas. In my topic, I believed there was no reason for analysing the way the information is communicated to the interviewer from the side of the speaker and thus, the data collection and analysis procedure relied on a clean verbatim style of transcribing.

The interviews followed semi-structured style with format being more relaxed and questions having more flexibility, depending upon the specific types of answers by the interviewees the interviewer had a chance to ask follow-ups or skip certain questions. Overall, the data collection procedure has included 12 questions for the interview and respondents were expected to answer the questions applying their own line of argumentation and looking from the personal perspective. The questions were semi-occupational (technical), and semi-idiosyncratic, meaning that while all the questions required some sort of knowledge on the field, not all of them were necessarily questions only specialists could answer.

Besides, the author of the thesis took into the account all aspects of the questions and issues which could cause problems with confidentiality and anonymity. While it asked for the consent of the respondents, the interviewees also had a right to have their names credited for the contribution they would give to the general research on the level of cyber security within E-Government of Azerbaijan. One of the respondents agreed for his name to be mentioned in the thesis while another respondent asked for anonymity which the researcher took into his consideration. While not all of the questions were answered with a special emphasis on state secret, occupation-irrelevant typology of the questions, the cumulative experience from the interviews could be deemed as successful and data gathered for this purpose will have a significant impact on the analysis of the current situation in Azerbaijani E-Government system and its future political implications.

4.3.1 Interview with Leading Cyber Security Specialist from EGDC

The first interviewee was Mr. Muhammad Rustamzadeh, the leading expert in the Cyber Security section of the institution called EGDC. The institution was created in the framework of National Strategy of the Republic of Azerbaijan on the Development of the İnformation Society for the years 2014-2020 and the main purpose of its foundation was to coordinate the transition to the new system of E-Governance and to enforce the supervision of the integration of the state institutions to the new system while passing through such transition process. He described his working environment and the overall situation in the management of cyber security challenges in the E-Government sector in Azerbaijan. His main points were that government in Azerbaijan are very attentive on this issue since the early 2010s and that there are many organizations, agencies and committees involved in the process of cyber-attack and cyber-crime prevention as government started allocating more resources not only for building the reliable cyber security framework, but also encourages universities to run cyber security classes. The main bodies he mentioned were Special State Protection Service of Azerbaijan (SSPS), which is now replaced by SSSCIS, CERT under MinCom, Main Department for Combating Organized Crime (MDCOC) of the Ministry of Internal Affairs (MIA) and State Security Service, which he elaborated, to be working together to eliminate the common cyber-criminal activities. One of the questions asked him about the main sources of threat to the agency servers which he responded that many hackers are targeting Azerbaijani as well as other Commonwealth of Independent States (CIS) governments since they are very vulnerable, to receive the data and get unauthorized access to the industrial control systems. He mentioned that many such attacks were performed from the Iranian domains and were aimed at either causing Denial of Service (DoS), or to capture the SCADA & ICS systems to get authorization for the energy and electricity control systems. Threats to disrupt such strategic public sectors worries the government and ensures that they take the issue of secure data storage in top-notch priority.

He also talked about the important presidential decree about the establishment of a Special Committee on Information Security in 2018 to monitor and watch closely the procedures of integration of agencies through the common system called X-Road. Mr. Rustamzadeh has expounded the advantages and disadvantages of using such a system for governance. Security was his personal priority and therefore, he mentioned that he likes the security parameters of the system while he also disclosed that there are huge complaints about the lagging nature of the system because it is sometimes very difficult to integrate state systems into it as the software updates are not being performed which causes a lot of criticisms of the system. He also contends that SSSCIS ruled it to be incompatible with the state cyber security legislation, as the system allows for unchecked and unverified transfer of the data between the intrastate agencies. In this light, Mr. Rustamzadeh has given us a small hint about the application of the brand-new system for E-Government called “ASAN” Bridge which was designed by the local specialists using the Google technology Kubernetes. He assures that the same problems will not happen under this very system as it was already tested for reliability by SSSCIS and the project is currently on the piloting stage.

4.3.2 Interview with Cyber Security Specialist from SAPSSI

Another interview conducted was from the cyber security specialist working in the State Agency on Public Service and Social Innovations under the President of Azerbaijani Republic. He kindly asked the authors of the thesis not to disclose his identity which was accepted. The same set of questions were asked to him regarding his opinion and knowledge of some facts about the cyber security policy framework in Azerbaijan. His main contribution was the information provided on the problems of the X-Road system. He asserted that the current administration of SAPSSI is not very satisfied with the system as it is designed to be a more liberal, decentralized rather than centralized system for E-Government. This issue causes the illegal transfers of data between the agencies without any requests and possibilities to monitor them. This is one of the main issues the SSCIS, as also mentioned by the previous interviewee, discusses and tries to resolve for the properly functioning legal framework for cyber security. Other shortcomings of the system, cited by the anonymous speaker, have been its inability to take huge amounts of data and integrate it smoothly into the state agency servers which leads to the lagging system. This process disrupts the intercourse between the agencies and prevents their operational work.

He also mentioned that Azerbaijani government has already set ready the national cyber security strategy to advance improvements and reforms on the works of the agencies with regard to their integration into the new system. He has stated that EGDC was established as a regulatory agency to coordinate the secure connection and communication channels between state agencies and organizations. He, like Mr. Rustamzadeh, told that the EGDC is working on the development of new system although he gave no details of the system but mentioned that the main reasons for the change of the system were the legal issues arising from the contradiction of the existing X-Road system to the cyber security laws of Azerbaijan. For instance, he mentioned that because X-Road was designed specifically for the organizational goals of Estonian government, the integration of the state agencies into it is a rather impossible job due to the incompatibility between the domestic political goals of Azerbaijani as well as Estonian governments.

4.3.3 Cross-sectional Design Interview Analysis

Drawing the lines between the answers given by the both specialists, it is easy to get yet a clearer picture about the situation in the current policy environment on E-Government as applied by the government officials. They both had agreed that Azerbaijan had been recently working very hard in the positive direction and described the situation with the future of the protection of cyberspace in the country as an achievable goal. The summarized points regarding the specific keyword-driven questions can be found in Table 1. While they both discussed the legal issues surrounding X-Road, Mr. Rustamzadeh was more passionately speaking about the cyber-attacks to the country internal systems as well as the nature and purposes of such attacks. What was an interesting contrast between the speakers was that while Mr. Rustamzadeh called Azerbaijani cyber security policies relatively new, anonymous interviewee mentioned the traditional internal agency security departments also as the part of the cyber security initiatives of the government. The main difference between their approaches is that point the former wanted to make was not that real cyber security practices did not exist in Azerbaijan, but that there was no government willingness over fixing the existing problems and political will came in 2011. This was one of the main explanations as to why cyber-security issues faced so much resonance lately.

Table 1. Cross-sectional Design Interview Results

Interviewees **Questions**	**Mahammad Rustamzadeh**	**Anonymous**
Occupation	Leading Specialist	CYBER SECURITY SPECIALIST
Timing of Cyber Security Policies	Relatively new, since 2011	Exists since the independence of Azerbaijan; internally managed traditional system
Intensity of Attacks	Politically-charged frequent foreign attacks from Iran	SAPSSI underwent no attacks

Current Government Policies	Special commission to monitor legal conflicts in X-Road	Policies to be announced after the NCSS is adopted
Organizations	CERT, SPS, MDCOC, SSPS	—
How SCISA SSPS works?	Regular monitoring; gap analysis of state agency servers	—
Cooperation	No such cooperation exists; banks usually cooperate with foreign companies	No foreign cooperation with SAPSSI; regular trainings abroad
Models	“ASAN” Bridge system	New system being prepared
X-ROAD Transition	Ideal system for E-Government; system is difficult to integrate/much lagging	Legal problems; limited server capacity; software update & integration difficulty
State Plans and Targets	Cyber security education at universities and training centres	National cyber security strategy
SAPSSI	E-Government system functions like ASAN Service	E-GOV is not new, since 2012; great achievements

4.4 Discussion

This section of the thesis delivers the rationale behind the whole idea of holding the study of cyber security challenges in one certain direction of Azerbaijani governance apparatus and reiterates the fundamental beliefs and assumptions of the thesis from the scratch, thereby giving the reader an understanding of the real sense of the research study and its practical applications. Furthermore, this section signifies the importance of the research for the construction of the solution packages aimed at building proposals derived from the conclusions of the research and serves as a transitional part by connecting results to the action plan.

To begin with, the thesis sought to establish the factors which affected and shaped the current policy outcomes in the cyber security structure of the E-Government in Azerbaijan. The thesis addressed the literature gap on the topic of inaugurating security infrastructure for E-Government in Azerbaijani cyber space. Thesis has raised the issues such as the problems within the Azerbaijani system for the protection of the strategic state information, the sources and the contexts of the occurrence of such problems, the ways in which the policy solutions could be improved and the models from the foreign experience which were applied in Azerbaijani E-Government system, and they are separately put forward in the paragraphs below for the purposes of independent analysis of the events that are interlinked to the central proceedings revolving around the key problems with the cyber security gaps of the state agencies.

The main difficulty which was not addressed before this research study was to understand which factors were causing the inefficiency of the government of Azerbaijan regarding the provision of security for strategic citizen as well as state data. The problem was identified as the mismanagement from the side of the authorities to prevent various cyber-attacks and cybercrimes targeted to disable state networks' full operation as well as their failure to secure rather more solid cyber security infrastructure. The evidence of the existing problems within the cyber security configuration of the E-Government was manifesting itself in the form of low scores in the world cyber security rankings such as Cyber Wellness Profile and National Cyber Security Index (NCSI), alongside with the fact that Azerbaijani governmental systems have been undergoing range of externally invasive and destructive attacks. These are proving the serious nature and urgent need of an immediate action directed towards finding the causes of problems and making necessary reforms to boost digital as well as political security of Azerbaijan. The results from the interviews can be detective of the persistent nature of attacks to the country's cyber space with malicious intentions to gain the access and control to the countrywide control systems of common energy and electricity grids, unauthorized subjugation of SCADA systems and the politically-charged landscape which shaped the terms conducive to the occurrence of such types. As such, the experts from EGDC and SAPSSI have provided their subjective analysis of the research questions posed by the thesis and delivered answers employed in the action plan sections of the thesis. Both the sources of the problem and the solutions to it are analysed in the twofold perspectives which allowed thesis to be gristly focused on finding the roots of the crisis prevailing over cyber security framework of Azerbaijan and decided to put an emphasis on the job of researching the rising opportunities for implementation of the new system for E-Governance. Interview results gave us yet additional perspectives and facts which are hidden from the internet and academic literature to understand how the cyber security decisions were taken inside the country.

As mentioned, Azerbaijan used to have no effective policy instruments and solutions directed toward the resolution of cyber security issues in the electronic governance systems of the country. However, as the authorities began to perceive the threats this could cause as well as the benefits that could be achieved through the operative strategies, the system of digital protection was ordered to be reinforced through the various defence mechanisms stretching from responding to the cyber troubles encountered by the civil users to the investigations of cyber-crimes happening on an international level. Before, no specific mechanism existed for the identification of cyber risks and the elimination of the wicked programs penetrated to the state systems for storing the data of citizens, systems for the control of energy systems, information on the state projects, and archives. The institution of separate entities and cyber response groups within the MinCom, MIA, SSSCIS and Azerbaijan National Academy of Sciences (ANAS) is the indication that the government position towards organizing defence of the country's cyber space was radically different than before. The graphs displayed in above sections also signposted the efforts and attention paid by the government toward the improvement and funding of the entities making up the national cyber security infrastructure. Increase in the government investment, budget allocation as well as creation of the new agencies for finding the answer to the challenges posed by the digital threats and risks are in themselves constitutive of state-encouraged actions toward changing the status and minimize the consequences of such risks.

The E-Government sector played the role of the main beneficiary and priority of the government since before the establishment of this system of governance there was no scheme for the storage of so much data in the single platform. Multidisciplinary principle of E-Government's work ensured that no operational control could be possible unless there is no central authority consisting of highly-profiled professionals governing the working environment and actions of the actors involved in the management of this structure. Therefore, as the next step EGDC's initiation contributed greatly to the advancement of the security and strategy for the government's vision on E-Government.

The foreign experience was one of the first strategies which authorities sought to apply in the country and the single partner country which Azerbaijan cooperated with was

Estonia whose model for e-governance experience was heavily used and applied into the local regime for e-governance. X-Road is the system that E-Government in Azerbaijan had been using since its starting times and as we could see from the interviews, Azerbaijan does not see it as an effective system for applying into the domestic electronic governance framework due to its conflict with the legal provisions regarding the transfer and requests of unauthorized materials and state documents / files in between agencies. Mr. Rustamzadeh explained that the government has launched the program for repealing the current system with the program tailored to their needs. Therefore, Google-made Kubernetes was selected as a template design system which had to be developed into the working E-Government system. As the testing shows, the program is successfully tested against the possible security malfunctions which means it is ready to be installed and integrated into the governmental systems and computers. Our thesis identified that the foreign investments are not necessary for the achievement of success here, instead, professional personnel and cyber security specialists are the keys for the government in this case. Together with the new system's application, the thesis also examined the desirability score of the several policy actions which could be followed in this way and the new system, which corresponded to the "rational" model of public policy making has outweighed others by a huge margin.

All in all, the thesis has managed to explore, discuss and elaborate on the problem of Azerbaijani E-Government's security, its reasons and context as well as propose the possible policy routes that are available for the application.

5 Policy Alternatives for Strong Cyberspace in E-Government

This section of the thesis addresses the proposals regarding the selection of the most desirable domestic policy actions on the improvement of the cyber security framework in practice of E-Government of Azerbaijan. The main method for such analysis which thesis undertakes is to present all the models at once in one section of the research study and later to compare those policy outcomes based on 5 criteria, which are effectiveness, efficiency, political viability (acceptability), equity and feasibility. We operationalize these criteria by defining them to let the opportunity to easily compare the outcomes when it comes to the selection of the most desirable outcomes. Multi-response desirability approach relies on the strength of thesis author's ability and skills to put forward his comprehensive analytical reasoning. As such, criteria themselves are asking the following questions:

- Effectiveness: Did the policy model achieve its intended outcome?
- Efficiency: Did the policy model use resources in the most utility-maximizing way?
- Equity: Did the policy treat its beneficiaries and stakeholders in the same way?
- Feasibility: Is this policy realistic in terms of implementation and can it be done in the current circumstances?
- Political viability: Will it be in line with people's interests and values? Will there be many people who would oppose the implementation of the new policy project?

5.1 Rational Model

The rational model of public policymaking concerns the application of new government policies specifically targeted at finding the final resolve to the problem and is designed to be cost-efficient when compared to the model which is decided to be repealed or replaced. Rational models are usually the ones which are brand-new for the existing policy schemes in the countries and those countries which decide that they do not wish to proceed with the same policy which they believe was lacking one or several of the components essential for policy. For example, the government may choose to proceed to the rational model of policymaking if it believes that the new model will fundamentally change the negative result gained from the conservative approach and aims at increasing direct benefits while decreasing the costs of implementation of a project.

In our case, government's policy which it could deemed as 'rational' is integration into new "ASAN Bridge" system. By integrating into the new system, the government does not only plan to reduce its information costs, but also grasp more control over the project and will be able to build a centralized data management system where it could regulate the proper flow and storage of the information and data. While the E-Government in Azerbaijan is utilizing the "X-Road" system designed in Estonia, it believes that the new system does not fit to the strategic and organizational needs of the country, so, it is believed that new system will be more effective (Anonymous, 2020). However, the effectiveness of the system is to be evaluated only after its implementation.

In terms of efficiency, with its reduced information costs, and reliance on Kubernetes technology which operates on Google servers and experience which had been trusted by many others in the governmental and business levels for its scalability, flexibility and mobility, it will also be an efficient option compared to "X-Road" that was a whole new system. In this case, state will not have to outsource specialists from the foreign country as it did in case of applying Estonian model, rather use its professional cadres and it will save the government an extra margin. Therefore, the system can be called an efficient one.

With regards to feasibility, we were informed that the system has already been tested by the SSSCIS and is expected to perform well when it is finally integrated to the state systems. Therefore, this project is also feasible, i.e. doable.

Equity parameter will have small laggings due to the internet user problems for small portion of Azerbaijani citizens. As it goes in the report of ITU, Azerbaijan had 79% of its population connected and actively using the internet in 2017 (ITU, 2018). In actuality, E-Government system is less for end users and more for government institutions' efficient working regime. And since the internet conncetivity is not a large-scale problem for the state agencies and institutions, the level of exclusion can be disregarded. Outcomes for this parameter will apply to any policy for E-Government as it applies to the rational model.

Political acceptability parameter demonstrates high result in this case, because not only government has approved the system, but also the technical tests and piloting stages of the project has been completed and even successfully passed the test of SSSCIS. This overall means that the rational model fully complies with the political acceptability criteria.

5.2 “Garbage Can” Model

“Garbage can” model refers to the old policies archived in the deepest corners of the state collections and used once in the public life, however, later removed from being implemented either because it failed to adapt to the old policy environment or because it had become obsolete over time. The main feature of this type of policymaking is that it applies the principle of “keep a thing seven years and you'll always find a use for it”, i.e. no policy is ever old-fashioned over the long term.

In our case, we will use the traditional Azerbaijani system used by the agencies to keep their computer networks intact and try to apply it to the E-Government system. If such approach would be possible, then there would be no understanding of the common system for all and thus, the feasibility part would cease to exist.

In terms of effectiveness, the policy of going back to the old system would neither deliver the results government expects from the implementation of such project, i.e. to ease the process of service delivery for the citizens and remove the operational communication barriers among the intrastate agencies when it comes to the transfer of the data necessary to implement certain tasks or projects as well as to securely store the data to prevent its acquisition from the unauthorized agents. In the old system, as Mr. Rustamzadeh mentioned, each organization was “organization own security” (Rustamzadeh, 2020). Since no centralized system existed, then it was both ineffective and inefficient policy for protecting the cyber space of the country from foreign attacks. Because when each agency runs its own cyber security independently, then it would be very challenging for the state to prevent the occurrence and reoccurrence of such attacks too the internal systems and much of the civic information would undergo massive thefts. Small nuance in efficiency would be that the traditional system would not cost much and this is a plus for efficiency parameter.

As to the political acceptability, this type of policy is neither acceptable for the governement, nor for the citizens. While the former wants to facilitate the operation speed of its services to the citizens, the latter would not accept that their data would be stolen by the third parties. This also would mean that the state fails to perform its strategic functions, security of its citizens’ information. Therefore, the traditional system fails the political acceptability test.

5.3 Status Quo

Status-quo is the policy choice directed to keep the existing state of the affairs and make little to no changes in the implementation of the certain policy projects. In our case, the current policy is the implementation of the X-Road system as a model for E-Government.

While the system was an “ideal one” for E-Government concerning its security potential, X-Road is an effective government policy to implement for the E-Government in Azerbaijan. However, as it was mentioned by both interviewees, the level of satisfaction by this system from the side of the government is considerably low due to its decentralized nature which was not intended. Therefore, it should be noted that while X-Road is an effective regime of security for E-Governance, it does not fully fit to Azerbaijani policy framework.

Regarding the efficiency, X-Road project, due to it being an outcome of foreign capital, is an initiative realized through outsourcing the IT security specialists from Estonia who have worked for high salaries. This means very high funds had to be spent for initiating a system through outsourcing when compared to the system built by the local specialists. So, project is not efficient to spend money on as there is a nice potential in local cyber security professionals to create one for the state for much lower payments and it will be easier to monitor the gaps in the system as the local professional lives in Azerbaijan and decreases communication and time costs.

In terms of feasibility, all the projects which have been implemented up to date, can be deemed as feasible because it means that they passed the workability barrier.

When it comes to the political acceptability, X-Road had small problems with the complaints by the end users because it sometimes prevented the fast operation of the system as integration to the system by the state agencies were not much smooth. The problem rather relied on the administrative mismanagement of the problem than real implications for non-acceptance of the policy. Therefore, X-Road is a politically viable option for the state.

5.4 Multi-Response Desirability Analysis (MRDA)

In this subsection, the author performs an analysis of the multiple responses through the application of the desirability approach towards the issue involving the selection of the most looked-for policy for the implementation in the next stage. This subsection juxtaposes the outcomes of the analyses conducted on the all available cyber security empowerment policies proposed by the thesis as different options and alternatives for upgrading the cyber security capacity of E-Government. The relative priorities given to the policies based on 5 criteria will be based on numerical scores. All criteria are regarded to be of the equal weight and one does not possess any differential effect on the policy than others. Scores are based on three types of preferential credits: full credit (1 point), partial credit (0.5 point) and no credit (0 points). Scores will be assigned based on the analysis provided to the content and the context of the policy solutions. Cumulative scores are displayed at the bottom of the Table 2. The policy with more points is assumed to become the policy option likely to be suggested.

In the multi-response desirability analysis “ASAN” Bridge project encoded as the rational model of policymaking, got the highest result, by scoring 4 out of 5 possible points and is the most desirable policy that the thesis would suggest according to the analysis of the findings, data and information gathered as well as composed into the single framework in the thesis. The lowest and least desirable policy is the system applied traditionally since the 1990s till 2010s by the state institutions, labelled as “garbage can” model with 1.5 points out of 5 points.

All in all, thesis agrees with the state strategy to implement the ASAN Bridge project into the E-Governance system as a way to enhance information security of state institutions and their data/information services.

Table 2. Desirability Analysis of the Policy Options

POLICIES CRITERIA	RATIONAL MODEL	"GARBAGE CAN" MODEL	STATUS-QUO
EFFICIENCY	1	0.5	0
EFFECTIVENESS	-	0	0.5
FEASIBILITY	1	0	1
POLITICAL VIABILITY	1	0	1
EQUITY	1	1	1
TOTAL SCORE	4	1.5	3

5.5 Study Limitations

Research study sought to present the renewed information about the current state of affairs revolving around the Azerbaijani state cyber response initiatives, involving the data collection performed in the framework of structured direct and structured indirect interviews and the analysis of the materials as was transcribed in the format of clean verbatim. Although the study encompassed an analysis of domestic policies which stuck to the objective social criteria, the new study needs to be carried out to reveal even more novelties and apply more mathematically measurable analysis of results to compare the weighted averages of the variables selected for the study.

The new perspectives are necessary to use the same action plan preparation but not just using 5 criteria for measuring the rate of success, but also collecting more statistical data to compare the relative superiority of these parameters. For that, we need to operationalize the criteria and put some indicators to become better able to lead the study to the conclusion about the most desirable outcome, while this thesis mostly conducted its analysis based on the explanatory comparison through fact-checking and subjective argumentation.

Another limitation of the study was associated with the insufficient number of interviewees due to the structural as well as unforeseen circumstances. As is mentioned in the methodology section, because of the absence of state information disclosure policies on the state's cyber security actions and projects. This leads to a situation where many state officials engaged in the issues directly related to such actions tend to refrain from sharing their knowledge and experience of the issues which could have contributed greatly to the research procedure. Secondly, due to the COVID-19 pandemic the research project was limited to the interviews which had to be conducted in virtual or audio format that could serve as a vulnerable environment against the information leakage or would put the confidential information under the risk of being obtained. Because of the limited nature of the data collection and interview gathering, the intended sample size considered for the research project could not be fully generated or reached and instead, the thesis focuses on obtaining common conclusions based on the full capacity that the interviews could possibly deliver.

5.6 Case of Georgia

As a country which locates within the region of South Caucasus, Georgia borders and shares much of its historical legacy with neighboring Azerbaijan. The experience of Georgia with the transition to the information society is happening in parallel to that of Azerbaijan's. The primary commonality between the two countries which allows us to reliably compare the case studies of the both is that they possess almost identical historical background with being under the influence of Soviet Union, being part of the Eastern Partnership Initiative (EaP), sharing similar characteristics regarding the GDP and population density size and so on. Given the similarity that exists between the nations, the interesting question that comes to one's mind is why Georgia is rather more successful in terms of integrating the e-government and achieving the higher standards of cyber security, not just by comparing its efforts on a regional but also on a global scale.

Currently, Georgia is easily a frontrunner of the region of South Caucasus when looking at the comparative scores of other countries' ranks in terms of the cyber security capacity implemented by the central government. According to the National Cybersecurity Index, a survey conducted by Electronic Governance Academy, Georgia is well ahead its neighbors with the index of 53.25 while Azerbaijan and Armenia have 37.66 and 31.17 points, respectively (Electronic Governance Academy, 2020). While providing similar rankings but different results, GCI, a survey by the ITU, ranks Georgia 18th in the world with the relative score of 0.857 while Armenia and Azerbaijan ranked 55th and 79th with the respective scores of 0.653 and 0.495. One may attribute such difference in results to the distinctive priorities on methods, however, both surveys show reliably accurate representations of the relative superiority of Georgia’s cyber security capacity when compared regionally. In order to find out the reason why the country with the background seemingly similar to that of Azerbaijan performs better, one should see the timeline of development.

The first time when Georgia was already sketching its plans for the integration of e-government was since 2003 when the “father” of Estonian e-government, Ivar Tallo, was invited to Tbilisi to the office of the George Soros Foundation where underlying topic was the discussion of e-government model applicable to Georgia (Tallo, 2016). The main challenge in the cooperation of Estonia and Georgia was the fact that not many people in Georgia did not believe that Estonian model would change things in Georgia since the population of the country was less cyber literate, the government was purely bureaucratic and lacked transparency which led them think this project would fail despite of the huge efforts put by the EU to sponsor such a transition (Israelyan, 2016). The main government motive behind the improvement of this structure was to increase efficiency and effectiveness in the work of the government as well as to boost economic development of the country by speeding up the legal processes which businesses faced in the light of the unproductive bureaucracy (Data Exchange Agency, 2019). As a result, started as early as in 2003, e-government initiative of Georgia delivered considerable wave of positive results as the digitization process cut costs and brought about beneficial projects which have built up citizen-centered model where the positive feedback loop contributed to the trust which helped the initiative flourish (Gvenetadze, 2014). Undoubtedly, one of the most successful ideas for the formation of positive G2C relationships was the project called “Public Service Hall” (House of Justice was its alternative name) launched by the inventiveness of the former president Michael Saakashvili (Public Service Hall, n.d.). This project was remarkable in that it facilitated the process of issuing whole range of governmental services from the receipt of the national ID card to the registration of the marriages. Interestingly, the identical model of providing government’s services based on “single-stop shop” (also called “single window”) principle was later applied in Azerbaijan by the SAPSSI through the brand name “ASAN” Service (Lent.az, 2012).

In our previously mentioned MRDA model, thesis has selected to proceed with the single rational choice option which assumed to bring in the policies that accounted for cost-benefit analysis and were innovative by its nature. It would not be redundant to mention that given Georgia’s close collaboration with Estonia and many other EU states like Italy Georgians are also safeguarding their computer networks and digital systems using rational choice approach by innovating their older infrastructure and transporting modern ideas based on the solid experience of EU states that are well-known with their digital literacy (Krabina, et al., 2012). With regards to the Georgian use of similar approach like Azerbaijan’s, it is worthy to mention that this fact allows us to conduct an overview of the two case study countries and provides an opportunity to study the possible differences in the policy routes which both governments have opted for. Apart from this, existing similarities in the backgrounds and policy choices of the two neighboring states represent a research strategy which is usually applied for the study of differences among the countries, most similar systems design (MSSD), that are being investigated from the same initial point and use inductive research as the way of depicting the sample from a systemic level (Anckar, 2008). This is not to say that thesis has been designed from the beginning to include the comprehensive MSSD comparative model for the examination of the research problem but rather it employed just some elements typical of MSSD model to understand the gap. In this sense, after the discussions around the reasons and strategies behind which Azerbaijani government was making decisions about its switch from the previously applied model (“X-road” prototype for the e-governance) to the more appropriate “Kubernetes” model, we would be in more of an advantageous situation that would play out for the analysis of Georgian model for cyber security in the e-government. As such the government of Georgia has cooperated with Estonia for the realization of the project and monitoring of the security measures considered for the new e-government platform. The Head of the Legal Department of Data Exchange Agency told the media that in the beginning of the project it was almost impossible to imagine that this cooperation on the initiative was hardly believed to deliver significant results (Goderdzishvili, 2017). The problem with this policy in Georgia was the lack of trust by the people in the process while Azerbaijan’s problem with the application of Estonia-powered X-Road system was linked to its incompatibility with the administrative goals of the government in the face of decentralization of the data processing and interagency relations management. Georgia, in turn, aimed at the reverse, to increase the efficiency of operations and delivery of the public services through the enactment of smaller dose of independence to those agencies.

Nevertheless, Georgia, being a state, which possesses almost identical historical background with Azerbaijan managed to hold ICT policies in such a way which helped it to better maximize the security of its networks than the neighbor despite the fact that they both seemed to advance the e-government structure equally. While looking into the timeline of the state ICT policies of many countries, we may observe a pattern that most of the advanced nations applying e-government later introduce comprehensive cyber security frameworks and strategies which serve to guide businesses and agencies dealing with the confidential information or the industries which operate critical infrastructures. This chronology order feels very intuitive since e-government is the primary driver of the demand for cyber security both from the side of the government and many businesses which are utilizing the services provided through e-government platforms. There is a model explaining such a phenomenon by linking the ICT development to the e-government and cyber security in a cyclical triad (Figure 3).

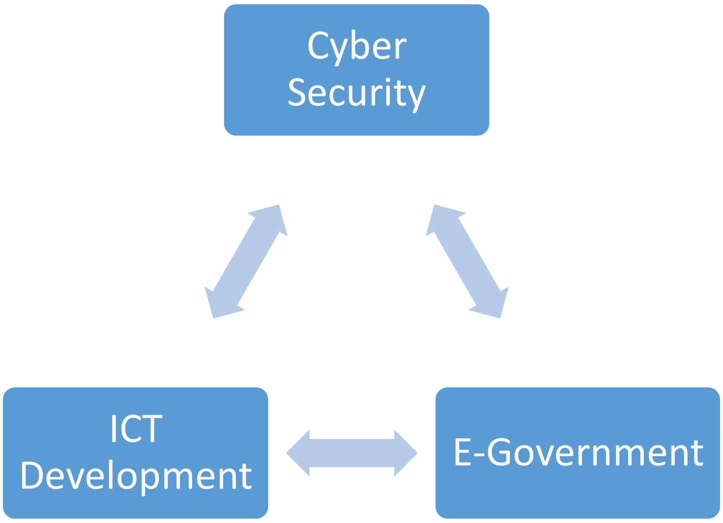


Figure 3. Cybersecurity, development and governance model

According to the mentioned model, these three phenomena serve as the mutual drivers and the approach assumes that e-government functions well only if cyber security system is well-organized (ITU, 2019). In this case, one reasonable explanation about the underperformance of Azerbaijani cyber security system emanates from this hypothesis: Azerbaijani government’s unwillingness to prioritize ICT field led to the massive cyber security underinvestment till 2011. However, one might still notice that even though Georgia began prioritizing this field way before Azerbaijan, they have comparable and somewhat equal performance in the sphere of e-governance, according to the EGCI 2020 (United Nations Department of Social and Economic Affairs, 2020). As we may observe from the Figure 4, Azerbaijan and Georgia have been steadily following one other's path during the observed time period and no considerable advantage persisted in any of the sides despite the fact that Georgia started investing heavily into the e-government infrastructure way before Azerbaijan did. Then one again might ask how does it happen that Azerbaijan is significantly outperformed in one field of ICT sector while other indicators are very responsive? Even though the timing of the investment seems to have the role in this phenomenon (because when Georgia invested in e-government before Azerbaijan, it already had already developed cyber security infrastructure), the fact that Azerbaijan is one of the ICT leaders among he CIS countries tells us that there is an extra reason to believe that cyber security performance gap between the two neighbouring countries (ITU, 2019). Looking at the ICT Development Index scores between Georgia and Azerbaijan (Figure 5), we clearly observe that Azerbaijan has been outperforming Georgia almost all the time since 2008 and it is to say that Azerbaijan in no way lags behind Georgia in the sphere of technology (ITU, 2016).

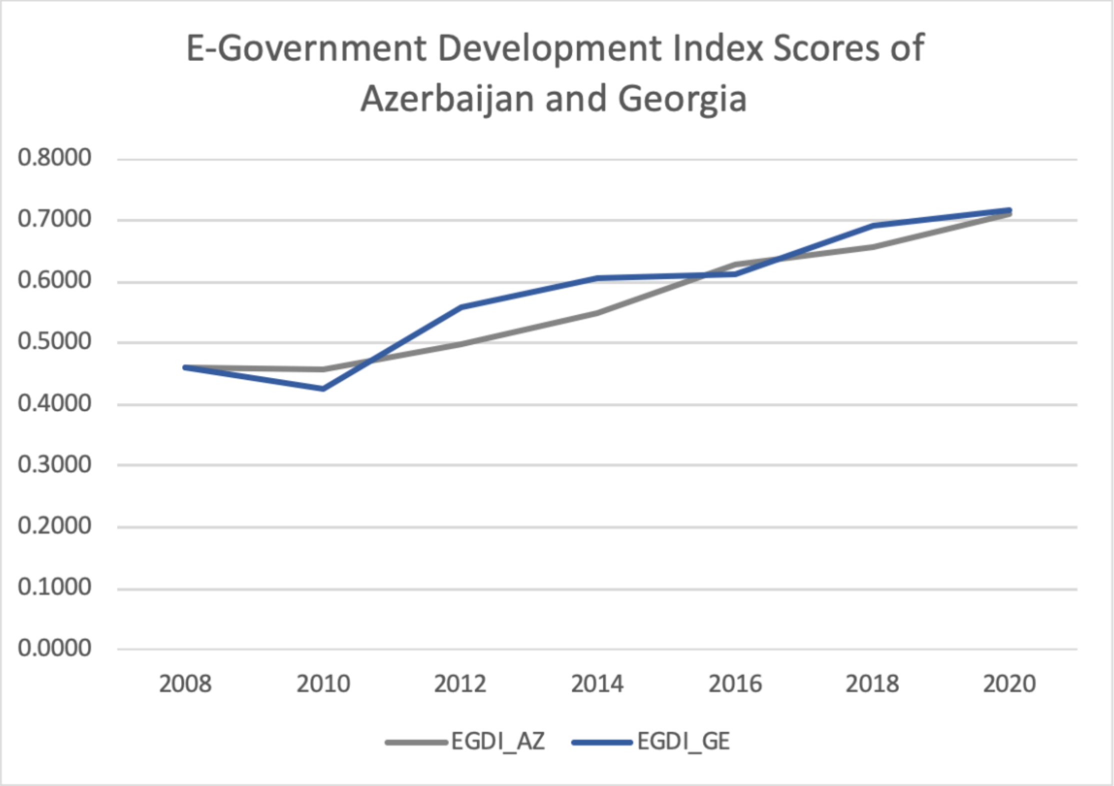


Figure 4. EGDI: Azerbaijan vs. Georgia

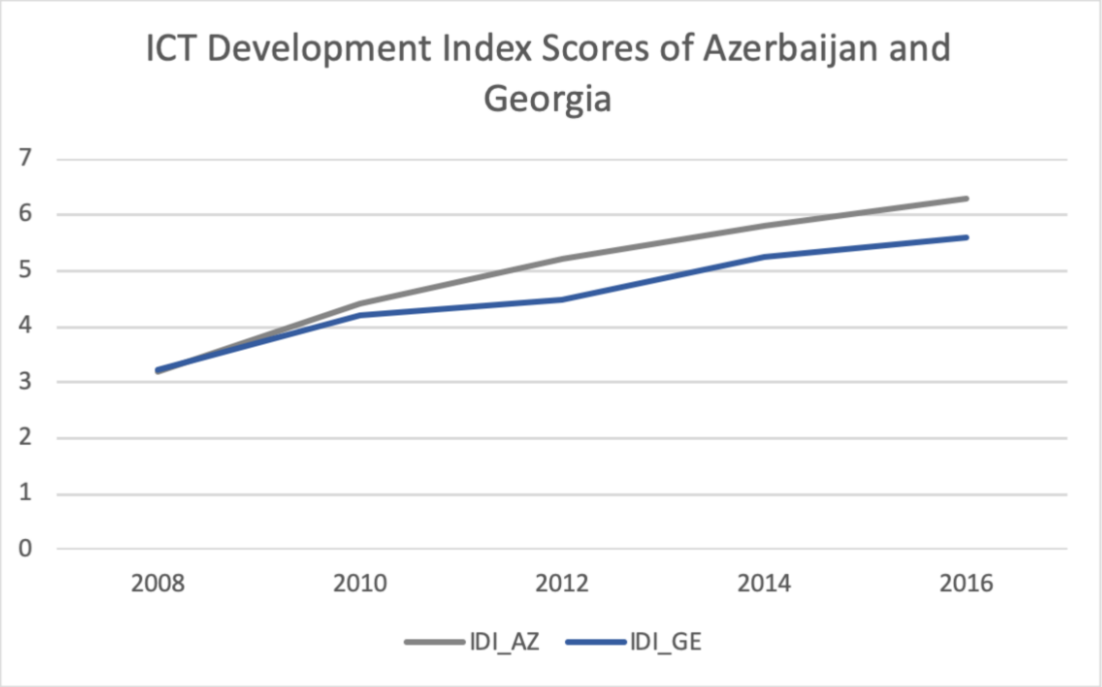
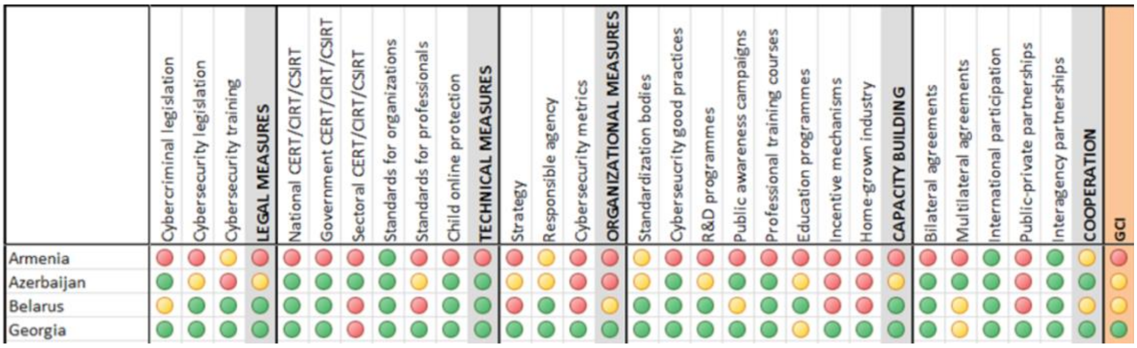


Figure 5. IDI: Azerbaijan vs. Georgia

However, Georgia’s relative overperformance can be explained by the “3-layer effect” which study has developed. Table 3 analyzes the timeline of the achievements and general figures representing the performance of both governments in terms of cyber security and e-governance to expressively contrast and juxtapose timing and the nature of the ICT policies as they were developed throughout the entire period discussed in the chapter. According to the proposal, Georgia was under the effect of 3 distinctive and self-reinforcing variables: the first one being the timing issue, the second being the large share of the private sector in Georgia and the third one being the DDoS attacks on critical infrastructure of Georgia during the cyber intervention from the Sandworm Team as Georgia was dragged into the state of conflict. While the first 2 issues are the results of the internal policies of the government of Georgia, the third “layer” of motivation was added to the government’s fear to lose control over the critical objects of within the country (United Nations, 2019). Azerbaijan, as a country, has also undergone similar attacks on its electrical utilities, power plants and pipeline operations as mentioned by our first interviewee (Rustamzadeh, 2020). These types of threats did not just provoke Azerbaijan to strengthen its cyber resilience platforms but also the same worked out for Georgia which cooperated with the NATO and the EU on the way towards improving its cyber security capacity to become almost the safest country within post-Soviet area (E-Governance Academy, 2017).



	Cybercriminal legislation	Cybersecurity legislation	Cybersecurity training	**LEGAL MEASURES**	National CERT/CIRT/CSIRT	Government CERT/CIRT/CSIRT	Sectoral CERT/CIRT/CSIRT	Standards for organizations	Standards for professionals	Child online protection	**TECHNICAL MEASURES**	Strategy	Responsible agency	Cybersecurity metrics	**ORGANIZATIONAL MEASURES**	Standardization bodies	Cyberseucrity good practices	R&D programmes	Public awareness campaigns	Professional training courses	Education programmes	Incentive mechanisms	Home-grown industry	**CAPACITY BUILDING**	Bilateral agreements	Multilateral agreements	International participation	Public-private partnerships	Interagency partnerships	**COOPERATION**	**GCI**
Armenia	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🟢	🔴	🔴	🔴	🔴	🟡	🔴	🔴	🟡	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🟢	🔴	🟢	🟡	🔴
Azerbaijan	🟢	🟡	🔴	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟡	🟡	🔴	🔴	🟡	🟢	🟡	🟢	🟢	🟡	🔴	🔴	🟡	🟢	🟢	🟢	🔴	🟢	🟢	🟡
Belarus	🟡	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🔴	🟢	🟢	🔴	🟢	🔴	🟡	🟢	🟢	🟢	🟡	🟢	🟢	🔴	🔴	🟢	🟢	🟡	🟢	🔴	🟢	🟡	🟡
Georgia	🟢	🟢	🟢	🟢	🟢	🟢	🔴	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟡	🟢	🟢	🟢	🟢	🟢

Figure 6. CIS region scorecard

Looking at the scorecard of the CIS countries on the Figure 6 from the report of the GCSI 2017, one may infer that Georgia has 5 components in which it outweighs Azerbaijan in the field of cyber security: cyber security training, cyber security metrics, incentive mechanisms, home-grown industries and public-private partnerships (ITU, 2017). Three of these phenomena (incentive mechanisms, home-grown industries and public-private partnerships) have direct link to one common conception which is the private sector development. The government of Georgia was launching the e-government project to revive and speed up the business activities to increase the economic welfare through raising the share of the private sector; consequently, private local companies started to boom and increase not only in scope but also their services expanded in quality. Today, most of the private information, critical infrastructure and other objects requiring solid cyber security system, almost 70%, are concentrated in the hands of the private sector in Georgia. This is in the large contrast to the real situation in Azerbaijan where cyber security is exclusively treated as state's strategic non-shared interest which is observed from the minuscule size of the private enterprises offering cyber security services, trainings and even courses. The main reason why there is so much gap between Georgia and Azerbaijan in the mentioned field is the primary responsibility of the 2nd layer, private sector's role in cyber security. In these terms, the absence of the positive correlation between the strengthened cyber security capacity and the expansion of the e-government as well as the ICT competence in Azerbaijan can be justified on the idea that the application and development of the e-government serves both governments' different goals and priorities. While Georgia made use of its e-government project to develop the speed and efficiency of the private business operations in the first place, Azerbaijani government realized this project more as an attempt to internalize the positive anti-bureaucratic effects of e-government systems, increasing the transparency within the governmental structures and therefore, increasing public trust in it.

Apart from developing home-grown industries and creating business incentives, government also fails to provide the conditions necessary for the presence of the popular cyber security trainings which could help to boost public awareness and increase the number of specialists in the field of information security. By creating incentives for the private sector, the government would also increase the risks and charges for the recipients of cyber security issues by making them build safer and organize more sustainable cyber infrastructure within the organizations' networks. This would be beneficial since then the demand for cyber security will skyrocket as more firms will be in need of organizing their own security in an attempt to avoid legal charges and fines for dismissive use of clients' private information or strategic utilities like that happened in Georgia which emphasized the essence of building the cooperation between the public and private sectors in its Cyber Security Strategy of 2012-2015 (National Security Council, 2012).

Table 3. Competitive Cross-Country Analysis

	Azerbaijan	**Georgia**
Adoption of the Legal Base for E-GOV	2010	2004
Establishment of the Main Body Regulating E-GOV project	2011	2010
Establishment of "single window" public service initiative	29 December 2012	26 May 2011
EGDI, 2020	0.71	0.7174
Maturity Phase of current E-Government	3rd	4th
Adoption of the Legal Base for Information Security	2011	2012
Cyber Security Strategy adopted on national level	2019-2024 (partially 2014-2020)	2012-2015
GCSI & NCSI, 2020	0.857 (18th); 53.25 (45th)	0.653 (55th); 37.66 (75th)
Public-Private Partnership	Low	High

International Cooperation	High	High
Public Awareness of Information Safety	Moderate	Moderate
E-Government Policy Approach	Rational	Rational

6 Summary

As it was stated many times, cyber security is one of the state priorities in Azerbaijan and with the technological improvement it gets ever more relevant to be able to protect strategic state information. The research study has focused on the cyber security problems in the sector of E-Government in Azerbaijan and the main purpose of the study was to investigate why there are problems in the field and what are the nature of such problems. Besides, the thesis analysed the qualitative data to reach at the decision with regards to the selection of the most desirable policy for the government of Azerbaijan in this sphere.

Study employed the qualitative methodology to find out the reasons of malfunctioning cyber security responses against the attacks from abroad, as well as the relatively lower scores of cyber-security sector in Azerbaijan. Study employed two methods for the analysis of data: content analysis method to reveal the reasons of the relative cyber-backwardness of Azerbaijan and interview method for divulging into the possible policy choices and disclosing the realities of Azerbaijani domestic policy environment while understanding the needs of a system which is going to be applied for intrastate agency communication. In the aftermath of conducting the content analysis and identifying reasons behind the security gap in the Azerbaijani cyber-infrastructure, study discusses that there was lack of cyber security strategy in the country which was reflected upon the other spheres of digital life in Azerbaijan as well. Those were legal framework, policy framework and education framework which were the segments affected by the absence of national cyber security strategy. What is more, those structures were, in turn, effectively diminishing Azerbaijan’s cyber-competitiveness against the rest of the world. Study elaborates on the historical facts from the periods of independent Azerbaijan and meritoriously demonstrates the timeline of its progress in this sphere which started after the beginning of the second decade of the 21st century, featuring government initiatives for cooperation with other states in the capacity-building process as well as introducing the facts about the existing cyber-infrastructure of Azerbaijan and its application on E-Government. As such the government actions should base their decisions taking into account the local e-government's standing in terms of maturity.

The interview procedure contributed to the designing of the action plan and suggestions to the government regarding the ways of improving the current state of affairs with cyber security development. After receiving the results, thesis suggested a model for application of the policies called multi-purpose desirability analysis model which contrasted 3 distinct policy tracks over effectiveness, efficiency, political acceptability, equity and feasibility criteria to have better odds of choosing the most in-demand policy action which government would most likely opt for pursuing. The rational model, represented by "ASAN" Bridge project, was selected as the most desirable policy alternative. Research study, overall, reached its goals but cyber challenges in E-Government system from different study perspectives should be the priority for researching.

The comparative analysis between Azerbaijan and Georgia served for the identification of the main differences between the two countries' cyber security systems and helped to reach out the conclusions on the state of the affairs in the policy preferences of each country and contributed to the research by helping to add new and necessary ideas for the action plan. 3-layer effect was mentioned as the main model for explaining the Georgia's advantage: timing, fear of the insecurity during the conflict and the extent of the private firms controlling the critical infrastructure and networks. As such the outperformance of Georgia's cyber security policies and capacity over Azerbaijan's was found to be attributed to the larger incentive instruments which the government of Georgia accounted for the benefit of the private cyber security firms' activities so that it created both an incentive for the better investment strategies within the mentioned sector as well as raising the requirements from the government towards the reliability of the such companies. Azerbaijan largely lacked such infrastructure and did not enjoy much of that productivity and performance growth which cyber security sector enjoyed in Georgia.

6.1 Answers to Research Questions

As a result of content analysis, the research study has found that the main reasons as to why there are problems with cyber security in the implementation of E-Government, I concluded that there is an involvement of several factors in the occurrence of deficiencies in the process of cyber security in the E-Government system. The main factors were those constituting the organizational foundation of the cyber security infrastructure in any countries. Study revealed that Azerbaijani authorities have failed to provide timely feedback to the gaps in the cyber space and that was reflected on the overall results, causing the structural factors which prevented the smooth functioning of the cyber security network in the country. Among those factors were the lack of the government willingness to carry out reforms in the digital sphere, absence of national cyber security strategy which would outline the cyber security framework in the central system, lack of legal framework on the issues of cyber security and its implementation terms until 2010s. There was the role played by the indirect factors such as the lack of strong cyber security and ICT education, small amount of domestic investments as well as the FDI in the mentioned field, high costs of infrastructure development and so on.

After the interviews were conducted, the proposed action plan was sketched and multi-response desirability analysis model was employed to compare the different policy routes and determine the most suitable one for the application into the E-Government system. In the end, rational model was chosen among three policy options and that model corresponded to the new project for repealing “X-Road” with “ASAN Bridge” system. The final analysis of the data brought thesis to the conclusion that the best policy model for the application will be the rational model, if to rely on the data and analysis provided in the thesis.

As for the comparative analysis, the research found out strong link between the level of engagement of the private sector with public sector as well as the size of the private sector and the strength of the cyber security capacity of the country when other variables affecting the outcome were controlled for. This accounted for the primary and largest difference which existed between the cyber capacity of Azerbaijan and Georgia. As such the necessity of the policies for the capacity building in the cyber security sector would have to involve the introduction governmental incentive systems and mechanisms to internalize the benefits of doing so.

6.2 Further Research

The topic of E-Government needs to be stretched out to include brand new ideas not just for the management of the cyber security policies of the Azerbaijani government regarding E-Government, but also on the effects of connectivity between all the various state apparatus and organizations on the overall security level of the data and information and to reveal the most desirable systems for making the idea of secure cyber space within the E-Government systems of Azerbaijan yet more feasible and safe. One possible issue that our study faced was that the websites, information platforms and media outlets which are open to the public do not release the transparent and accountable reports regarding the policymaking issues and standard operating procedures followed within the organizations in charge of providing the cyber security of the information systems used in the e-governance. We, as researchers were not able to talk to many representatives of such organizations and gain huge amount of information on the subject since the issues of cyber security were deemed as state secret and thus, the operations of the ministries and the agencies adjacent to them were either rarely reachable or there were too many limitations preventing the objective researching environment.

Alongside with researching the administrative process, it would be feasible to measure the digital literacy or cyber awareness/preparedness of the local people in Azerbaijan instead of focusing on the evaluation of the policy making techniques and strategies of the policymakers. Inclusion of more case studies than just single example like this thesis did through the method of most similar systems research design on Georgia and Azerbaijan would better be improved by the inclusion of the most different systems research design on a comprehensive scale to find out the similarities Azerbaijan's case demonstrates with those of countries coming from the different and alien to Azerbaijani system and background. This would help us to better adhere the correlation between the digital literacy and the results of current cyber-awareness test demonstrated by Azerbaijan. New study areas within the administrative plan should, therefore, be considered and applied in the future.

References

ABC. (2019, March 12). *Bu gün Bakıda Beynəlxalq "Kibertəhlükəsizlik həftəsi" öz işinə başladı*. Retrieved from ABC: http://abc.az/mobile/view.php?id=24464&lng=az

Ada, S., Sharman, R., & Gupta, M. (2009). Theories Used in Information Security Research: Survey and Agenda. In R. Sharman, & M. Gupta, *Social and Organizational Liabilities in Information Security* (pp. 279-292). Hershey: IGI Global.

Adliyya. (2013, October). Application of advanced ICTs within the judicial system is the center of attention. *Adliyya*, p. 10.

Alguliyev, R., Yusifov, F., & Gurbanli, A. (2018). Methodology and Criteria for Evaluating E-Services: The Case of Azerbaijan. *Journal of E-Democracy*, 106-115.

Aliyeva, Z. (2015, April 10). *Cyber security in Azerbaijan*. Retrieved from Newtimes: http://newtimes.az/az/cyberspace/3441/

Alizadə, S., & Aliyev, B. A. (2018). Kibertəhlükəsizlik dövlət təhlükəsizliyinin tərkib hissəsi kimi. *ЮРИДИЧЕСКИЕ НАУКИ И ОБРАЗОВАНИЕ*, 21-29.

Anckar, C. (2008). On the Applicability of the Most Similar Systems Design and the Most Different Systems Design in Comparative Research. *International Journal of Social Research Methodology* , 389-401.

Andersen, K. V., & Henrisken, H. Z. (2006). eGovernment maturity model: extension of the Layne and Lee model. *Government Information Quarterly*, 236-238.

Anonymous. (2020, May 9). Cyber Security Policies in E-Government. (I. Huseynov, Interviewer)

Asadli, J. (2018). PROPOSING ACTION PLAN IN CYBER SECURITY CAPACITY BUILDING FOR AZERBAIJAN. Tallinn, Estonia: TALLINN UNIVERSITY OF TECHNOLOGY Department of Software Science School of Information Technology.

Asan Imza. (2018, January 28). *Azerbaijan has become the first country to implement the prototype of Estonian X-Road platform in e-government system*. Retrieved from Asan Imza: https://asanimza.az/news-en/2018/azerbaijan-has-become-the-first-country-to-implement-the-prototype-of-estonian-x-road-platform-in-e-government-system_en/

ASAN Radio. (2019, July 19). *Afghanistan wants to benefit from Azerbaijani experience in cyber security*. Retrieved from ASAN Radio: http://www.asanradio.az/news/24624

Awoleye, O. M., Ojuloge, B., & Siyanbola, W. O. (2012). Technological Assessment of e-Government Web Presence in Nigeria. *ICEGOV '12* (pp. 236-242). Albany: ACM.

AZCLOUD. (2020, July). *AZCLOUD Data Center*. Retrieved from AZCLOUD: https://azcloud.az/en/view/about/

Bakutel. (2012). *BAKUTEL 2012: IT SECTOR - NEW TRENDS*. Retrieved from Bakutel: https://archive.bakutel.az/2012/?l=en

BBC. (2013, December 2). *Əli Abbasov: Kiber hücumlara bəzi hökümətlər dəstək verir*. Retrieved from BBC: https://www.bbc.com/azeri/azerbaijan/2013/12/131202_cybersecurity_bakutel

Bergman, S. (2012). Pakistan's Route Closures Have Tripled Transportation Costs. *Inside the Pentagon*, 6-7.

Big Policy Canvas. (2018, November 23). *X-Road*. Retrieved from Big Policy Canvas: https://www.bigpolicycanvas.eu/community/kb/x-road

Brajshori, B. (2017). Public policy analysis and the criteria for evaluation of the public policy. *European Journal of Economics, Law and Social Sciences*, 50-58.

Burton, J. (2013). Small states and cyber security: The case of New Zealand. *Political Science*, 216-238.

Cabinet of Ministers of the Republic of Azerbaijan. (2013, March 28). *Action Plan on the announcement of 2013 as the "Year of Information and Communication Technologies" in the Republic of Azerbaijan.* Retrieved from E-Qanun: http://e-qanun.gov.az/framework/25505

Cabinet of Ministers of the Republic of Azerbaijan. (2014, April 2). *National Strategy of the Republic of Azerbaijan on the Development of the İnformation Society for the years 2014-2020*. Retrieved from President of the Republic of Azerbaijan: https://president.az/articles/11312

Cabinet of Ministers of the Republic of Azerbaijan. (2014, February 10). *State Program of the Republic of Azerbaijan on development of the protection of the state secret for years of 2014-2018*. Retrieved from E-Qanun: http://www.e-qanun.az/framework/26965

CERT Azerbaijan. (2020). *E-Security Service*. Retrieved from CERT: https://cert.az/xidmetler.html

CISCO. (2017). *Cybersecurity scholarship opens career opportunities in Azerbaijan*. Retrieved from learningnetwork.cisco.com: https://learningnetwork.cisco.com/s/it-success-story/a2E3i0000009UvqEAE/sabina-hasanli

Conklin, A., & White, G. B. (2006). e-Government and Cyber Security: The Role of Cyber Security Exercises. *39th Hawaii International Conference on System Sciences,* (pp. 1-8).

Crandall, M. (2014). Soft Security Threats and Small States: the Case of Estonia. *Defence Studies*, 30-55.

Data Exchange Agency. (2019). *E-GEORGIA: Decades of Successful Transition.* Tbilis: Ministry of Justice of Georgia .

Department of Public Relations of State Security Service . (2017, December 30). *Information of the Department of Public Relations of State Security Service* . Retrieved from State Security Service : http://www.dtx.gov.az/news188.php

Dhakal, G., Amatya, P., & Bal, B. K. (2012). Trust Issues in the E-Government Implementation in Nepal. *ICEGOV '12* (pp. 524-525). Albany: ACM.

E-Gov Development Center. (2020, March 3). *Elektron Hökumət üzrə İcra Qrupunun Kibertəhlükəsizlik alt Qrupunun ilk görüşü keçirilib*. Retrieved from E-Gov Development Center: https://www.digital.gov.az/az/media/news/elektron-hokumet-uzre-icra-qrupunun-kibertehlukesizlik-alt-qrupunun-ilk-gorusu-kecirilib

E-Governance Academy. (2017, June 8). *eGA contributed EU twinning project in Georgia*. Retrieved from E-Governance Academy: https://ega.ee/news/ega-contributed-eu-twinning-project-in-georgia/

E-Governance Academy. (2018). *Situation Review: Safety and Security of Cyberspace and E-Democracy in the Eastern Partnership Countries.* Tallinn: e-Governance Academy.

E-Governance Academy. (n.d.). *National Cyber Security*. Retrieved from E-Governance Academy: https://ega.ee/cyber-security/

Elamiryan, R. G., & Margaryan, M. G. (2018). Cyber Security in the Context of Armenia-NATO Cooperation. *Journal of Information Warfare*, 99-111.

Electronic Governance Academy. (2020). *Ranking Timeline*. Retrieved from NSCI: https://ncsi.ega.ee/compare/

European Parliament. (2017, February 25). REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON ENISA (THE EUROPEAN UNION AGENCY FOR CYBERSECURITY) AND ON INFORMATION AND COMMUNICATIONS TECHNOLOGY CYBERSECURITY CERTIFICATION AND REPEALING REGULATION (EU) No 526/2013 (CYBERSECURITY ACT). Strasbourg, France.

Farajova, A. (2019). E-government implementation challenges: case studies and views. *APPLICATION of INFORMATION and COMMUNICATION TECHNOLOGIES* (pp. 18-19). Baku: ADA University.

Foreign & Commonwealth Office; National Cyber Security Centre; The Rt Hon Dominic Raab MP. (2020, February 20). *UK condemns Russia's GRU over Georgia cyber-attacks*. Retrieved from The Government of the UK: https://www.gov.uk/government/news/uk-condemns-russias-gru-over-georgia-cyber-attacks

Gafarbayli, T. (2015). E-signature and Cyber Security. *Second Republican Scientific Conference on the Multidiciplinary Problems of Information Technologies* (pp. 150-152). Baku: Ministry of Transport, Communication and High Technology.

Goderdzishvili, N. (2017, March 2). From Georgia to e-Georgia: a robust transformation as it happened. (U. University, Interviewer) Retrieved from United Nations University: https://egov.unu.edu/news/news/from-georgia-to-egeorgia-robust-transformation-as-happened.html

Gvenetadze, I. (2014). *Georgia's Successful Journey to E-Government: E-Government Development in Georgia.* Retrieved from Center of International Technical Aid of the EU for Belarus: http://cu4eu.by/upload/iblock/22b/22bfb531435cd68b11c6f3a603289abd.pdf

Hasanli, E. (2015). Information Security and National Interests of the Republic of Azerbaijan in the Age of Globalization. *2nd Republican scientific conference on multidisciplinary problems of information security* (pp. 30-32). Baku: Institute of Information Technologies of National Academy of Sciences of the Republic of Azerbaijan.

Herzog, S. (2017). Ten Years after the Estonian Cyberattacks: Defense and Adaptation in the Age of DigitalInsecurity. *Georgetown Journal of International Affairs*, 67-78.

Hitchens, T., & Goren, N. (2017). *International Cybersecurity Information Sharing Agreements*. Center for International & Security Studies.

Horne, C. A., Ahmad, A., & Maynard, S. B. (2016). A Theory on Information Security. *Australasian Conference on Information Systems* (pp. 1-12). Wollongong: ACIS.

İmamverdiyev, Y. (2013). Milli kibertəhlükəsizlik strategiyalarının analizi. *İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı* (pp. 14-17). Baku: AMEA İnformasiya Texnologiyaları İnstitutu.

International Telecommunication Union. (2014, August 12). *CYBERWELLNESS PROFILE AZERBAIJAN.* Retrieved from itu.com: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Azerbaijan.pdf

Ismailzade, F. (2020, July 28). Retrieved from Facebook: https://www.facebook.com/fariz.ismailzade/posts/10163713167420398

Israelyan, Y. (2016, August 23). *Estonian experts: "Georgia has made a huge leap in e-government".* Retrieved from Digital Report: https://digital.report/estonskie-ekspertyi-gruziya-elektronnoe-pravitelstvo/

ITU. (2016). *Measuring the Information Society Report 2016.* Geneva: ITU Publications.

ITU. (2017). *Global Cybersecurity Index 2017.* Geneva: ITU Publications.

ITU. (2018). *Measuring the Information Society Report Volume 2 2018.* Geneva: ITU Publications.

ITU. (2019). *Global Cybersecurity Index (GCI) 2018.* Geneva: ITU Publications.

ITU. (2019). *Measuring the Information Society Report Volume 2 2018.* Geneva: ITU Publications.

Janczewski, L. J., & Caelli, W. (2016). *Cyber Conflicts and Small States.* New York City: Routledge.

Jongman, B. (2017). Recent Online Resources for the Analysis of Terrorism and Related Subjects. *Perspectives on Terrorism*, 150-181.

Joshi, A., & Tiwari, H. (2012). Security for E-Governance. *Journal of Information and Operations Management*, 254-257.

Krabina, B., Liu, P.-W., Meyerhoff-Nielsen, M., Millard, J., Reichstädter, P., & Wimmer, M. A. (2012). *A Digital Georgia e-Georgia strategy and action plan 2014-2018.* Retrieved from Digital Exchange Agency: https://dea.gov.ge/uploads/eGeorgia%20Strategy.pdf

Layne, K., & Lee, J. W. (2001). Developing fully functional e-government: a four stage model. *Government Information Quarterly*, 122-136.

Lent.az. (2012, September 6). *The structure of the State Agency for Public Service and Social Innovations is approved*. Retrieved from Lent.az: https://news.lent.az/news/101541

Makili-Aliyev, D. K., & Attiq-ur-Rehman. (2013). *CYBER-SECURITY OBJECTIVE: AZERBAIJAN IN THE DIGITALIZED WORLD.* Baku: Center for Strategic Studies.

Mammadov, B. (2005). Legal framework of ensuring of cyber security in the Republic of Azerbaijan. *ITU WSIS Thematic meeting on Cybersecurity for the Information Society.* Geneva: Ministry of Communications and Information Technologies.

Mammadov, B. (2008). Legal framework of ensuring of cyber security in the Republic of Azerbaijan. *Cooperation against Cybercrime.* Strasbourg: Ministry of Communications and Information Technologies.

Maric, M. (2014). E-Government 3 Web Security Issues: Who, What, When? In A. Vaseashta, P. Susmann, & E. Braman, *Cyber Security and Resiliency Policy Framework* (p. 176). Herndon: IOS Press.

Ministry of the Education of the Republic of Azerbaijan. (2020, February 6). *Charter on the establishment of the Board of Trustees within the higher educational institutions.* Retrieved from E-Qanun: http://e-qanun.az/framework/44427

Ministry of Transport, Communications and High Technologies of the Republic of Azerbaijan. (2019, June 3). *Presidential Decree on the creation of the G-Cloud and measures on the introduction of cloud services*. Retrieved from E-Qanun: http://www.e-qanun.az/framework/42560

Ministry of Transport, Communications and High Technologies. (2020). *II International "Cyber Week"*. Retrieved from Cyber Week: https://cyberweek.az/index_en.html

Ministry of Transport, Communications and High Technology of the Republic of Azerbaijan. (2016). Strategic Roadmap for the development of telecommunications and information technologies in the country. Baku, Azerbaijan.

Mission of the Republic of Azerbaijan to NATO. (n.d.). *Emerging Security Challenges* . Retrieved from Mission of the Republic of Azerbaijan to NATO: http://nato-pfp.mfa.gov.az/en/content/44

Molnar, A., Janssen, M., & Weerakkody, V. (2015). E-Government Theories and Challenges: Findings from a Plenary Expert Panel. *Conference: International Conference on Digital Government.*

Morgus, R., Fonseca, B., Green, K., & Crowther, A. (2019). *Russia and Cyberspace.* Washington: New America.

National Assembly of the Republic of Azerbaijan. (2010, May 11). *The Law on Private Information of the Republic of Azerbaijan.* Retrieved from E-Qanun: http://www.e-qanun.az/framework/19675

National Security Council. (2012). *Cyber Security Strategy of Georgia 2012-2015.* Retrieved from ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Georgia_2012_National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf

NCSI. (2020). *Methodology*. Retrieved from National Cyber Security Index: https://ncsi.ega.ee/methodology/

Panahov, H. (2016). Cyber-security challenges in Azerbaijan. *Baku Dialogues*, 1-6.

Pawlak, P. (2018). Protecting and defending Europe's cyberspace. In N. Popescu, & S. Secrieru, *HACKS, LEAKS AND DISRUPTIONS: RUSSIAN CYBER STRATEGIES* (pp. 103-114). European Union Institute for Security Studies.

Priisalu, J., & Ottis, R. (2017). Personal control of privacy and data: Estonian experience. *Health Technology*, 441–451.

Public Service Hall. (n.d.). *About Us*. Retrieved from Public Service Hall: http://psh.gov.ge/main/page/7/405

Qafqazinfo. (2020, March 16). *Special State Protection Service is abolished*. Retrieved from Qafqazinfo: https://qafqazinfo.az/news/detail/xususi-dovlet-muhafize-xidmeti-legv-edildi-280842

Respublika. (2019, February 12). *İqtisadiyyatın inkişafında İKT sektoru prioritet sahələrdən biridir*. Retrieved from Respublika: http://www.respublica-news.az/index.php/iqtisadiyyat/item/21773-igtisadiyyat-n-inkishaf-nda-ikt-sektoru-prioritet-sahaelaerdaen-biridir

Roguski, P. (2020, March 6). *Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace*. Retrieved from Just Security: https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

Rustamzadeh, M. (2020, May 5). Cyber Security Policies in E-Government. (I. Huseynov, Interviewer)

Savoldelli, A., Codagnone, C., & Misuraca, G. (2012). Explaining the eGovernment Paradox: An Analysis of Two Decades of Evidence from Scientific Literature and Practice on Barriers to eGovernment. *ICEGOV '12* (pp. 287-296). Albany: ACM.

Schläpfer, M., & Volkamer, M. (2012). The Secure Platform Problem Taxonomy and Analysis of Existing Proposals to Address this Problem. *ICEGOV '12* (pp. 410-418). Albany: ACM.

Singh, S. (2011). E-Governance: Information Security Issues. *International Conference on Computer Science and Information Technology* (pp. 120-124). Pattaya: ResearchGate.

State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan. (2020, July 30). *Accountability Module of the Intellectual Monitoring System*. Retrieved from State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan: http://vxsida.gov.az/statistics/

State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan . (2012, July 13). *Presidential Decree on the institution of the State Agency for Public Service and Social Innovations under the President of the Republic of Azerbaijan* . Retrieved from E-Qanun: http://e-qanun.gov.az/framework/24212

Tallo, I. (2016, August 28). Georgia has made a huge leap in e-government. (Y. Israelyan, Interviewer)

Transparency International. (2015). *E-GOVERNMENT AND E-SERVICES IN AZERBAIJAN CURRENT STATUS AND PROSPECTS (JANUARY-JUNE 2015).* Baku: Transparency Azerbaijan Fight Against Corruption Public Union.

United Nations Department of Social and Economic Affairs. (2020). *E-Government Survey 2020 Digital Government in the Decade of Action for Sustainable Development With addendum on COVID-19 Response.* New York: United Nations.

United Nations. (2019, August). *Report of Georgia on Resolution 73/27 on Developments in the field of information and telecommunications in the context of international security Resolution 73/266 on Advancing responsible State behavior in cyberspace in the context of international secur*. Retrieved from United Natiions: https://www.un.org/disarmament/wp-content/uploads/2019/08/georgia-73-27-73-266-dea-mod.pdf

Verdiyev, Ə. (2018, July 4). *Kibertəhlükəsizliyin əsasları, texnologiya və vacib olan nüanslar*. Retrieved from Ordu.az: https://ordu.az/az/news/135746

Xəbərlər. (2014, November 12). *Kiber savaş: gülləni kim atacaq?* Retrieved from Xəbərlər: https://xeberler.az/new/details/kiber-savas:-gulleni-kim-atacaq--7867.htm

Yoon, S. (2019). *Azerbaijan: Country Digital Development Overview.* Mandaluyong: Asian Development Bank.

Zulfigar, F. (2020, March 5). *Azerbaijan needs a systematic education program on cyber security*. Retrieved from TED: https://ted.az/az/view/news/13900/azerbaycanda-kibertehlukesizlik-uzre-sistemli-tedris-proqrami-yaradilmalidir-ndashachiqlama-nbsp

Appendix 1 – Interview Questions

1. Since when do the government work towards improving the information security in the country?

2. What are the main challenges recognized by the state as the factors of threat to information security in Azerbaijan in terms of e-gov?

3. Were there many organized cyber-attacks which could pose potential danger to the confidential governmental documents/files?

4. What are the current government policies aimed at improving the level of national cybersecurity from Cyber-attacks?

5. Which organizations are the most important ones in fight against cyber-crimes happening in the virtual space of the Republic of Azerbaijan?

6. What are the working principles of Special Communication and Information Security State Agency of the Special State Protection Service of the Republic of Azerbaijan? How does it organize the work of COMPUTER EMERGENCY RESPONSE CENTER (CERT) and AzScienceCERT?

7. Is there any organization which we are cooperating with to ensure the smooth transition to the improved systems of cybersecurity?

8. Which models are there which Azerbaijan aims at following in the event of pursuing comprehensive cybersecurity framework policies? Does Estonia provide a nice example for following?

9. How useful was the transition process towards the X-road on the way of organizing secure data transfer through the collaboration with the government of Estonia? Which challenges did you face when implementing this project?

10. What are the current goals and targets of the state in ensuring the information security of the country? Which preparations are being done for the next 5 years? (legislation, laws, conventions, policies, agreements, contracts, etc.)

11. What are the some of the achievements you managed to secure as the transition was processed very recently? How efficient and effectively is E-Gov working under the supervision of SAPSSI?