ADA University

SCHOOL OF PUBLIC AND INTERNATIONAL AFFAIRS

MASTER OF ARTS IN DIPLOMACY AND INTERNATIONAL AFFAIRS

CAPSTONE PROJECT

Comparative Analysis of the Legislation of the EU Countries on the Regulation of Critical information Infrastructure

Latif Nabiyev, Havva Orujova, Samra Mansimli

Baku,

Azerbaijan

May 20, 2023

PROGRAM: Master of Arts in Diplomacy and International Affairs

STUDENTS' NAMES: Latif Nabiyev

Havva Orujova

Samra Mansimli

APPROVED:

Faculty Supervisor: ________________________

Organization Supervisor: ________________________

Dean of the School: ___________________________

May 20, 2023

STATEMENT OF AUTHENTICITY

I have read ADA’s policy on plagiarism and certify that, to the best of my knowledge, the content of this paper, entitled *Comparative Analysis of the Legislation of The EU Countries on the Regulation of Critical Information Infrastructure,* is all my own work and does not contain any unacknowledged work.

Signed: Latif Nabiyev
Signed: Havva Orujova
Signed: Samra Mansimli

May 20, 2023

Abstract

Critical Information Infrastructures are an integral component of contemporary society, encompassing indispensable services that form the foundation of our daily existence, such as healthcare, energy, water, and transportation. Given its vitality to societies, it has become a major concern for national security, as many governments strive to ensure that these infrastructures are not disrupted, or much worse, subject to debilitating cyberattacks. The present capstone project makes a comparative examination of the legislative frameworks governing the regulation of Critical Information Infrastructure in the European Union member states and Azerbaijan, while also looking into the experiences of other countries. The study has revealed that at the time of preparing the paper, the biggest issue in the Azerbaijani legislation pertains to the new national cybersecurity strategy that has been subject to many negotiations that have delayed its approval; however, there are other amplifying issues pertaining to the lack of cybersecurity specialists, lack of public awareness on cybersecurity, and limited research and development. To help the institutions compensate for the lack of guidance as brought about by the lengthy approval process, the project proposes the government to lay the preliminary groundwork for the critical information infrastructure protection, promotes research and development in cybersecurity, takes the necessary measures to increase public awareness on cybersecurity through inclusion of courses in curricula, and adopting certain international cybersecurity standards. The options are weighed against one another according to the five main criteria. Overall,

Keywords: Critical Information Infrastructure, Critical Infrastructure, Azerbaijan, EU, Cybersecurity, Legislation, Türkiye.

Table of Contents

List of Abbreviations

CEN	Committee for Standardization
CENELEC	Committee for Electrotechnical Standardization Abbreviation
CERT	Computer emergency response teams
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical information infrastructure protection
CIP	Critical infrastructure protection
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act
CISA	Cybersecurity & Infrastructure Security Agency
ECCC	European Cybersecurity Competence Centre
EPCIP	European Programme for Critical Infrastructure Protection
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
FSS	Federal Security Service
ICS	Industrial Control Systems
ICT	Information and Communication Technology
IDDA	Innovation and Digital Development Agency
IEC	International Electrotechnical Commission
ISA	International Society of Automation
ISO	International Organization for Standardization Abbreviation
ITU	International Telecommunication Union’s
MDDT	Ministry of Digital Development and Transport
NIS	Network and Information Security Directive
NIST	National Institute of Standards and Technology
SPS	Science for Peace and Security
XRITDX	State Service for Special Communication and Information Security

Chapter 1. Introduction

The prevalent use of Information and Communication Technology (ICT) is, without doubt, the most defining characteristic of the modern world, as it has revolutionized the way we lead our lives and interact with others. Seeking to benefit from their application, countless, if not all, governments have taken significant measures to expand on their use and have thus paved the path for the realization of many ambitious projects. However, as the world keeps expanding the horizons of technological innovation, it is also opening the path for many critical security considerations.

Although ICT has laid the ground for an increasingly technological and interconnected world, its extensive use has also rendered many societies critically dependent on them. To illustrate the case, one needs to look no further than their implications for critical infrastructure (CI). Alcaraz and Zeadally (2014) define CI as the combination of physical and virtual assets and systems that are so essential to a nation that any disruption in the provision of their services could endanger their national security, public safety, and economic well-being. These disruptions can be the results of many factors, the most important ones ranging from natural force majeure events to terrorist attacks. Although each country or bloc has a peculiar conception of CI, the European Union (EU) defines critical infrastructure in its European Programme for Critical Infrastructure Protection (EPCIP), where it classifies them as being related to energy, *information and communications technology,* water, food and agriculture, healthcare and public health, financial systems, civil administration, transportation systems, etc. For this paper, one needs to delve deeper into the ICT component of critical infrastructure, which has become the sole guarantor of the proper operation of many other sectors mentioned above. This is where Critical Information Infrastructure (CII) comes in. The International CIIP Handbook (2009) defines CII as material and digital assets, networks, services, and installations, which – if disrupted – can have cascading consequences for the security and well-being of a country, as well as the government's ability to function properly.

At this point, it is important to clarify the relationship between CI and CII. Despite there being countless opinions on this matter, it is plausible to assume for now, and for the foreseeable future, that the two concepts are interrelated, in the sense that discussions on critical infrastructure protection (CIP) almost always inadvertently end up in discussions on critical information infrastructure protection (CIIP) (Dunn, 2005, as cited in Markopoulou & Papakonstantinou, 2021).

Today's societies cannot go a day without employing ICT, which is why many believe they have become more vulnerable. In this context, this sort of vulnerability refers to their susceptibility to a wide range of cyber threats that know no borders, and this is an especially alarming matter when it comes to CIs. According to the Digital Defense Report prepared by Microsoft (2022), last year's cyberattacks targeting CIs constituted 40% of all nation-state attacks; this rate went up at the outset of the war in Ukraine. In the case of the US, the Federal Bureau of Investigation (FBI) reported that in 2021, the Internet Complaint Center received over 600 complaints about ransomware attacks targeting the country's CI. Over the past several years, most of the cyberattacks have been targeting the Industrial Control Systems (ICS) that are in charge of keeping CI operations under control. The reasons, as Markopoulou & Papakonstantinou (2021) argue, are a) the potential of inflicting great damage through such attacks and b) the vulnerabilities of the ICS. Given the interrelatedness of multiple CIs, a disruption in one can have grave consequences for others.

In this regard, upscaling the CI resilience against cyberattacks has been at the centre of many nations' policymaking for many years now. For instance, in the case of the EU, the protection of CIIs was an utmost priority in 2009. That was when the EU Commission adopted the CIIP Action Plan, which later laid the groundwork for the Network and Information Security (NIS) Directive. The directive encouraged member states to drive the much-needed changes in their *national cybersecurity strategies* by introducing measures that would ensure vulnerability management and cyber hygiene. As of now, in addition to the revised NIS known as NIS2 Directive, the EU also has established the Directive on Resilience of Critical Infrastructure, otherwise known as the CER Directive (European Commission, 2022). The latter requires the member states to identify critical actors in 11 predefined sectors, who must in turn take measures laid out in its text (Confederation of European Security Services, 2022). The case of the EU alone serves to show that the protection of CIs, and cybersecurity in general, continues gaining a foothold in policymaking, especially in the post-COVID-19 pandemic world.

As previously mentioned, cyber threats know no geographic boundaries, and every nation can fall prey to their repercussions. In this regard, one must also consider Azerbaijan's activities in the area. A good place to start would be referring to international performance indexes. In 2020, Azerbaijan ranked 40th among 194 member states in the International Telecommunication Union's (ITU) "Global Cybersecurity Index," scoring a total of 89.31 points (ITU, 2021). This score also placed Azerbaijan third in the CIS region, following Kazakhstan in the 2nd and Russia in the 1st place. However impressive the ranking may seem, one needs to look within the state to understand its organizational structure and the latest developments taking place. Going back to as early as 2012, the State Agency for Special Communication and Information Security of the Republic of Azerbaijan and the Cyber Security Center under the Ministry of Digital Development and Transport of the Republic of Azerbaijan (MDDT) were established as institutions in charge of information security in the country. Based on the Decree No. 957 on "the improvement of management in the field of special state protection," the same State Agency became State Service for Special Communication and Information Security (XRİTDX, in Azerbaijani). Likewise, in 2018, the Coordination Commission on Information Security (İnformasiya Təhlükəsizliyi üzrə Koordinasiya Komissiyası) was established by Presidential Order No. 3851 to ensure the security of information systems and resources of the infrastructure important to the state and society from cyberattacks. More importantly, however, the State Security Service (DTX) and XRİTDX were appointed as the relevant institutions in ensuring the CII security, based on Presidential Decree No. 1315 (2022).

In addition, there is a number of computer emergency response teams (CERT) that operate in Azerbaijan in accordance with international standards. The National CERT (www.cert.az) functioning under the MDDT serves as a coordinating body whose main purpose is to detect and take preventive actions against cyber threats. There is also a Computer Emergency Response Center (www.cert.gov.az) operating under the XRİTDX that is tasked with managing the security of networks of public institutions. Further, AzScienceCERT (www.sciencecert.az) is yet another CERT that deals with matters related to the National Academy of Science's network security.

The policy problem as of now concerns Azerbaijan's cybersecurity strategy. The Coordination Commission on Information Security has already agreed with the relevant institutions on the content of the draft of the National Strategy of the Republic of Azerbaijan on Information Security and Cyber Security for the period 2023-2026. Although the strategy is expected to give additional impetus to the cybersecurity development in Azerbaijan, it has yet to be approved. Just like any other country, Azerbaijan is susceptible to a variety of cyber threats. Since cyber has no tangible boundaries, any malicious act perpetrate done within the domain can surely target Azerbaijani users and assets. Referring to Microsoft's report above, the reason for such an inflated percentage of cyberattacks targeting CI was the war in Ukraine. By bringing an example of the worsening US-Iran relations, Bruce (2022) argues that attending to CI security is especially important when one is engaged in an international conflict. Similarly, Lewis (2018) argues that the world is witnessing the growing role of cyberattacks during times of interstate conflict – a phenomenon that is likely to be become more pervasive in the future.

With that in mind, one can see how this can turn out to be a problem for Azerbaijan. To this day, the country is experiencing sporadic hostilities with Armenia, all while engaging in slow-paced peace negotiations rendered ineffectiveness by Armenian intransigence. At the outset of the 44-day war of 2020, Azerbaijan quickly fell prey to a series of cyberattacks, most of them launched by an unidentified group using the so-called "PoetRAT Malware" (Talos, 2020). Although the perpetrators targeted the VIPs in the public sector, the situation could have been far more serious had they targeted the country's CIs.. Since national cybersecurity strategies are to guide governments in upscaling their cyber resilience, any delay in their enactment and implementation may render CIs vulnerable to constantly emerging cyberattacks. In their Guide to Developing a National Cybersecurity Strategy, the ITU (2021) contends that the implementation part of national cybersecurity strategies is essential, as they set government objectives and identify the measures that need to be taken so to achieve them. Ergo, considering the debilitating effects that cyberattacks can have on society if targeted at CI, any delay in the approval of national strategy can leave Azerbaijan open to a vast array of threats and preclude the government from being able to effectively contain the situation. With that in mind, both the government and society are primary stakeholders in the CIIP.

The purpose of this paper is to examine current state of the legislation on the CIIP in Azerbaijan, as well as those of other countries (e.g. the EU member states, the US, Russia, Germany) leading in this scene, and propose courses of actions to the institutions in charge of the CIIP to implement, both in short and long terms. Because Azerbaijan's national cybersecurity strategy is currently in the process of approval, the institutions in charge of cybersecurity do not have a guiding document that establishes the key priorities and standards procedures for them to follow. This problem is further aggrandized by lacking capacities in areas pertaining to public awareness, research and development, and management of the CIIP, all of which are essential for bolstering the country's overall cybers security capacity.

That is, by examining the practices of focal countries, the paper will offer insights into how and on what bases have other countries devised their legislation. The ultimate purpose is to provide the institutions in charge of the CIIP and the MDDT with a variety of policy options that can be implemented in Azerbaijan so as to develop a congruent plan for upscaling its overall cyber resilience.

1.1 Methodology

The following study largely employs qualitative research approach to make a comparative analysis of the legislation on the CIIP among the EU member states and contrast them with what is currently being done in Azerbaijan. However, the analysis is not limited to the EU only, as it also looks at how other countries like the US and Russia manage the CIIP. However, due the nature of the current paper, the findings of these analyses had to be discussed within the framework of the current developments and challenges in Azerbaijan. Since this area is subject to constant change, the authors of the capstone project organized meetings with the experts from the Ministry of Digital Development and Transport of the Republic of Azerbaijan (MDDT) to gain better understanding on the current developments. At the same time, in order to collect primary data, the authors likewise participated in the two events on the CII, organized and attended by the representatives of the institutions in charge of the country's cybersecurity, as well as a number of international experts from companies like CISCO that delivered speeches and engaged in lengthy Q&A sessions. These events were:

- Seminar on "Critical Information Infrastructure Protection: National and International Aspects" that was held by the Association of Cybersecurity Organizations of Azerbaijan (AKTA) on April 6, 2023;
- Online conference on "Cybersecurity & Digital Transformation" held by Bako Tech on April 20, 2023.

In these events, the authors of the project listened to the presentations delivered by representatives of public institutions such as the AKTA, MDDT, XRITDX, and DTX , while also taking part in discussions that were happening on a Q&A basis. This approach helped the authors gain more primary data.

On top of collecting primary data, secondary data was also aggregated by referring to academic articles covering matters related to cybersecurity in Azerbaijan, as well as many other countries such as the ones in the EU. During research, the main focus was on national strategies, earmarked for developing the resilience of CII across different countries including Azerbaijan. However, given that the problem is extremely multifaceted, the research also focused on other areas of relevance to the CIIP, such as the importance of building the necessary human capital, advancing the research and development activities, raising public awareness, all of which was to serve the betterment of Azerbaijan's capacity in this area. In this regard, these sources proved helpful in carrying out the comparative analysis between the countries and supporting the options proposed to the institutions in Azerbaijan.

Although there is a plethora of literature on this field in a global context, there exists only a handful of studies that look into the CIIP in Azerbaijan. Most of the available literature are outdated and at best provide cursory analysis without delving too much into details; this has made it difficult to acquire valid data for the comparative analysis. That said, this is the only considerable challenge that is limiting research in this area.

The capstone project consists of five chapters that look into different aspects of the policy problem at hand. Chapter one includes the introduction, as in choosing this exact topic and the motives behind chosen matter, along with the methodology that describes how the study was carried out. Chapter two looks into the current policy problem in Azerbaijan from different angles – of which there are four – each with their own analysis. Furthermore, chapter three serves provides alternative policies that the project deems necessary for the government to implement. The chapter likewise looks into the experiences of other countries in order to support the rationale behind the options. Chapter four significances the factual and foremost option that could be considered as an alternative in the short term. Finally, chapter five includes the conclusion and endorsements about the options for the policy problem that is discussed throughout the paper.

Chapter 2. Problem Description

As far as the world is concerned, the biggest challenge in cybersecurity today comes with the constant need to adapt to the newly emerging cyber threats. To address the emerging challenges, governments face the need of constantly introducing new policies. This is particularly crucial when it comes to safeguarding critical information infrastructure, which – if disrupted – can inflict lasting damage to a nation. Realizing this, many governments have started shaping their national strategies to ensure their protection. However, even these have to be renewed every once in a while. In general, however, in order to see the current cybersecurity hindrances in Azerbaijan or anywhere else, one needs to take heed of the following factors:

- Legislation;
- Education and Public Awareness;
- Human Capital;
- Research & Development.

The significance of these factors lies in their contribution to the country's long-term cybersecurity capacity development, making them key priority areas for 2023 (from the speech of SA from the IDDA during the conference on cybersecurity and digital transformation, 20 April 2023). One may even go on to argue that these factors determine the content of national strategies and policies for cybersecurity, which is why they are of utmost importance to many governments across the world.

The lengthy process of negotiating the strategy is in itself an obstacle, as the document is supposed to serve as a guiding document for government agencies to consult at all times Be that as it may, an ever greater problem is posed by the absence of sufficient legislation needed for further development of the protection of the Azerbaijani CII. The development will not take place without an effective legislation, which will serve to encourage public institutions to adhere to certain CIIP standards and procedures (from personal communication with LK from the MDDT, 3 April 2023).

2.1 Lack of regulatory framework on developing the Critical Information Infrastructure Protection

As of now, the biggest challenge in developing the Azerbaijani critical information infrastructure protection pertains to legislation, specifically the national strategy. As previously mentioned, the Coordination Commission on Information Security has already prepared and submitted the draft of the "National Strategy of the Republic of Azerbaijan on Information Security and Cyber Security for the Period 2023 – 2026." However, the document has yet to come into force, which is why this process in itself has several implications for the CIIP development.

Firstly, the fact that the process is taking long inhibits the further development of the national CIIP measures. After all, the country's strategy was prepared to serve as a guiding document for institutions to refer and coordinate the joint efforts in upscaling the national cyber resilience. According to Ghernouti-Helie (2010), a national cybersecurity is created to establish a coherent approach of cybersecurity that is enforceable on a national level and compatible with international practice. Similarly, it is argued that without a national cybersecurity strategy, the government organizations will not be able to establish a clear picture of the upcoming developments and duties (from personal communication with LK, 3 April 2023). That is due to the fact that the document both outlines the necessary measures that the government has to take until 2026 and determines the duties of institutions in charge of overseeing national cybersecurity. Therefore, drawing on all of the above, one would not be wrong to assume that without enacting an effective national cybersecurity strategy, it is near to impossible for a government to properly organize the work of its mandated institutions and put forward a cohesive approach for handling emergencies.

Secondly, one must consider the current post-war environment in the region. As a result of the Second Karabakh War, Azerbaijan and Armenia engage in dragged out negotiation processes and occasionally resort to violence either at the border or in the region of conflict. Referring to Bruce (2022), a country must be especially wary of cyber threats when it is involved in international conflicts. That is because in this day and age, belligerents are inclined to target each other's CI as a way of wearing each other out and dealing a decisive blow to a nation as a whole. Coming back to the document, however, the strategy features guidelines and standard procedures that are to be followed in times of cyber incidents (from personal communication with LK from the MDDT, 3 April 2023). Ergo, in case there is ever a fallout in negotiations between Armenia and Azerbaijan, and the countries resort to an armed conflict, Azerbaijan may not be able to withstand the next round of cyberattacks, or at least mitigate its effects in a way that minimizes the damage made. In other words, because there is always a chance that an adversary launches a series of debilitating cyberattacks on CIs. the situation in the Azerbaijani context demands the government's most urgent attention.

On top of all of the above, the national strategy in question contains a clause on upscaling the national CII resilience for the period 2023-2026 (from personal communication with LK from the MDDT, 3 April 2023). According to the ITU (2021), national cybersecurity strategies are help safeguard CI and CIIs from cyber threats by devising a clear risk-management approach that is to be employed by mandated institutions. Ergo, it is fair to assume that the national cybersecurity strategy of Azerbaijan could at present provide guidelines for institutions to follow and use to build a base for further developing the country's CIIP.

2.2 Lack of Public Awareness on Cybersecurity

Before introducing any changes to the current state of cybersecurity, especially the development of critical information infrastructure protection, in Azerbaijan, one needs to address the elephant in the room – public awareness on cybersecurity. Granted, developing legislation and national strategy on this matter is undeniably important; however, the targeted audience has to have a proper understanding of what critical infrastructure protection, and cybersecurity in general, entails. In the case of Azerbaijan, this problem is largely unresolved, as the level of public awareness on cybersecurity to this day still remains low (from the speech of the EB from AKTA during the seminar on the CII, 6 April 2023). The reason why it is important for the current case is because the targeted audience for the legislation or national strategy on CS has to have sufficient understanding of the field and the CII in order to be able to adhere to their provisions and in turn maximize their security (from personal communication with LK from the MDDT, 28 April 2023). Therefore, without attending to this matter, any attempt at driving changes in the current CIIP will fall short of their objective, which is maximizing their security for the long-term period.

Since 1995, Azerbaijan been actively working with its international partners through the NATO Science for Peace and Security (SPS). However, it was after 2014 that the public sector workers in Azerbaijan were provided with advanced cybersecurity training courses. In their report, the NATO SPS editors (2022) argue that there is an insufficient level of cybersecurity awareness in Azerbaijan and that not enough is being done in terms of education or research in this area. This argument is very much akin to the one made by the representative of the MDDT, as it touches upon the potential danger of cyberattacks targeting CII in Azerbaijan. As far as the argument goes, there is a relatively low threshold for launching cyberattacks on the ICS, which is why they will most likely remain part of future conflicts (NATO SPS, 2022). As can be surmised from this, this factor becomes especially problematic in the case of Azerbaijan where cybersecurity awareness to this day remains low, and the country is stuck in an endless loophole of negotiations and occasional flare-ups with its neighbor.

Another worrying aspect of the lack of awareness on cybersecurity pertains to the most common types of cyber-attacks that target Azerbaijan. During his speech at the Fintex Summit that was held in Baku on June 16, 2022, the Head of the CERT under the XRİTDX reported that phishing attacks, social engineering, and website cloning constitute the most common types of cyberattacks that are directed at Azerbaijan (Trend News Agency, 2022). What is important to note that is that phishing attacks target individuals, as they seek to gain their personal information by seeming as legitimate corporate emails or messages. Furthermore, in 2022, around 10,000 ransomware attacks were reported as having been launched at the Azerbaijani internet information resources (from the speech of SA from IDDA during the conference on cybersecurity and digital transformation, 20 April 2023). This, in turn, has a big say in the critical information infrastructure protection. According to Back and Guerette (2021), the European Cyber Security Perspective 2019 holds the human factor to be on the par with technology development in protecting the critical information security, which is why increasing cybersecurity awareness is important for minimizing losses that can come as a result of cyberattacks.

In this regard, the extensive use of phishing as a popular method of cyberattacks targeting the country can have severe repercussions, following that they can be used to gain access to sensitive info such as login details and other access credentials and then be used to sabotage a CI. Being problematic as it is, this issue can be further aggrandized if victims lack sufficient internet usage experience, are technology-ignorant, or are simply naïve enough to fall prey to such attacks (Ghaffir et al., 2018). One must note that this issue is a global problem, as many countries – even the significantly developed ones – often become victims of such attacks. A well-known example would be Korea Hydro & Nuclear Power Co. – a CI – which nearly succumbed to the phishing attacks launched at their retired employees. What happened was that the perpetrators bypassed all the security measures in the CIIP and employed something known as “social hacking” (Min, 2017). What this means is that the group that launched the attacks had acquired sensitive information about the retired employees and then tried to use them to gain access to the CII. Therefore, considering what has been postulated so far, the lack of cybersecurity awareness in Azerbaijan can be especially potent if left unaddressed, especially considering that human-centered cyberattacks remain a majority.

2.3 Lack of the Human Capital in Cybersecurity

In the face of growing cyber threats around the world, countless governments are investing great resources in order to bring up the necessary cybersecurity culture in their domestic settings. Akin to its international counterparts, Azerbaijan faces the same, if not bigger, risks of falling prey to cyberattacks in the near future. In this regard, the task of developing Azerbaijan’s cybersecurity capacity is further complicated by the shortage of national cybersecurity professionals (from the speech of EB from AKTA during the seminar on the CII, 6 April 2023). These are the experts that possess the ability to help institutions reduce the negative consequences caused by cyberattacks by leveraging their knowledge to pinpoint weaknesses and create tactics that can minimize their effects. What is interesting to note that this issue seems to have remained unresolved. When one considers Azerbaijan’s National Strategy for the Development of the Information Society in the Republic of Azerbaijan for 2014-2020, they can discover that its guidelines contained a clause on promoting cybersecurity education among the population and institutions, as well as providing training opportunities for personnel specializing in this area (Spînu, 2020). It would thus seem that not enough has been done to promote professional cybersecurity culture, which may explain why there is still an issue of the lacking cadre specializing in this area.

A similar claim was made by the former director of the ICT Lab: Application and Learning Center who stated that there were not enough cybersecurity professionals in Azerbaijan (Trend News Agency, 2020). According to the co-founder of ThriveDX – the leading global institution specializing in cybersecurity capacity-building – Dan Vigdor (2023), the lack of cybersecurity professionals can result in huge gaps in security, which can further lead to irresponsible handling of personal data or utter collapse of important infrastructures. It is for this reason that AKTA strives to attract the Azerbaijani youth to cybersecurity through many workshops that it organizes (from the speech of EB from AKTA during the seminar on the CII, 6 April 2023).

Although the problem is said to have greater repercussions in the Azerbaijani context, it extends well beyond the country. According to the International Information System Security Certification Consortium's (ISC)^2 Cybersecurity Workforce Study (2022), there is a need for more than 3.4 million cybersecurity professionals, as the demand for experts in the area is greater than ever. One could argue that the demand has surged following the COVID-19 pandemic when many governments opted for digital solutions. The same applies to Azerbaijan that amplified its use of ICT during the special quarantine regime. This is to say that Azerbaijan may now be more susceptible to cyberattacks than ever before.

2.4 Limited Research and Development in Cybersecurity

Another problem that comes along with the existing impediments relates to the limited domestic R&D in cybersecurity. For starters, it is worth mentioning that Azerbaijan is among the leading countries in terms of using pirated software (from the speech of EB from AKTA during the seminar on the CII, 6 April 2023). According to Microsoft (2016), the main problem that emanates from the widespread use of unlicensed software is that cybercriminals exploit them to spread malware and expose users to a multiplicity of security risks. Exploiting user downloads, cyber criminals often bundle Trojans with the software so as to increase the chances of their execution and thus infecting the victim's computer. In order to rectify this problem, the government is planning to increase the development of domestic software that are eligible for certification and widespread use throughout the country; however, the greatest hurdle in the way concerns the limited research and development opportunities, which again comes back to the lack of sufficiently competent IT professionals (from the speech of EB from AKTA during the seminar on the CII, 6 April 2023).

Currently, the Cybersecurity Center under the MDDT serves as the leading institution in the cybersecurity R&D (from personal communication with LK from the MDDT, 28 April 2023). Apart from providing training opportunities, the center is gradually turning into an institution in charge of carrying out the national R&D. Despite these developments, however, it is too early to judge whether the center will be able to give impetus to the national research and development in cybersecurity. However, the issue as it remains poses a challenge, as it is also linked with the lacking human capital in cybersecurity. That is, the lacking R&D in cybersecurity is further aggrandized by lack of capable cybersecurity cadres.

Overall, one can see that the question of strategy is multifaceted, in the sense that the country's capacity to manage its CII also depends on factors other than legislation. So far, the findings indicate that Azerbaijan does not have sufficient number of cybersecurity cadres and is rather limited in terms of driving R&D in this area. More than that, however, there is an even greater problem of the limited public awareness, which exposes the country to different cyberattacks. In short, however, it becomes clear that even if the national strategy is approved, there are other aspects that the institutions must attend to in order to give force to the legislation.

Chapter 3. Policy Alternatives

For the time being, the institutions in charge of the CII assets in Azerbaijan must work collaboratively to devise a preliminary action plan or at least prepare to undertake certain measures to bolster the CIIP. This, in itself, entails that the government does the following:

- Adopt certain regional CII standards in Azerbaijan;
- Create a register of all CII assets functioning in the country and arrange them based on the criticality factor;
- Prepare a blueprint for the management CII management, including the security and monitoring mechanisms;
- Raise public awareness.

3.1 Adopting CII Standards in Azerbaijan

Aside from the issue of the pending approval of the national strategy, there is also a matter of standardization. Being highly dynamic, the current cybersecurity landscape places a great importance on developing certain standards and enforcing them. According to Srinivas et al. (2018), developing cyber security standards is essential, in the sense that they allow a government to enforce certain requirements that are to be adhered to by various state bodies. More specifically, cyber security standards enable institutions to manage cyber risks by determining basic security requirements, utilize the most effective practices in the field, enhance their operations, and access interchangeable technology as a result of minimized technical variations (Scarfone, 2009). Therefore, one of the policy options in this case is to adopt a set of regional CII standards, which can be used to promote professional capacity of the institutions (e.g. operators) and to strengthen the critical information infrastructure protection of the country. To do so, the mandated institutions must consult the regional standards for the CII operations have them confirmed through the usual governmental procedures. To this date, Azerbaijan has developed 59 standards in ICT based on the international ones (MDDT, 2021). However, it has neither created, nor adopted standards on the CII. For this reason, it is advisable for the government to adopt standards on the organization of CII functions in the country, which will lead to a significantly bulwarked CIIP and certifications. Whether Azerbaijan should create its own standards or adopt the already available ones is not up to a question, as there is currently insufficient that accommodation their creation.

As of now, there is an overwhelming need to develop a set of standards in order to lay the ground for an effective critical information infrastructure protection in Azerbaijan. Without enforceable standards, it will be impossible to ensure that operators take the appropriate measures to mitigate potential risks, let alone implement the needed technology in a proper manner (from personal communication with LK from the MDDT, 28 April 2023). That is, in the absence of standards, the CII operators may unknowingly implement the technology that is replete with vulnerabilities; this may in turn jeopardize protection of the whole CII asset. In this regard, the current policy option suggests developing a set of enforceable CII standards that will serve to increase the CII resilience in the country. The idea is to endow CIIs in Azerbaijan with a minimum required level of cybersecurity, which is to be achieved by calling on the operators to organize their work along such standards.

Today, there is a variety of standards developed by numerous countries and international organizations. In the case of the EU, there are a few important organizations that specialize in developing cybersecurity standards. These are the European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI). According to Gorniak et al. (2019), the CEN and CENELEC standards are not usually free, whereas it is the opposite with the ETSI whose standards and technical reports are free of charge. Regardless, both organizations strive to create standards that are also applicable globally, with the ETSI having a membership of over 900 organizations from 60 countries (ETSI, 2023). Overall, these organizations are tasked with supporting the creation of European regulations and legislation, as well as relevant standards through consensus. Coming to the standards themselves, however, Gorniak et al. (2019) argue that the ISO/IEC JTC 1/SC 27 – which was developed as a result of a close cooperation between the CEN-CENELEC Joint Technical Committee, the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC) – is to be deemed as the first reference in cybersecurity standards. Another noteworthy example is the National Institute of Standards and Technology (NIST) based in the US that provides guidelines and standards for organizations to minimize cybersecurity risks. However, the NIST is mostly known for its cybersecurity framework, which is essentially based on the "identify – protect – detect – respond – recover" approach.

Since operations of the CIIs are continuously being enhanced through system automation, which Marshall et al. (2018) claims enhances efficiency, Azerbaijan may consider opting for international standards like the ISA/IEC 62443 that deals with securitization of such processes. According to the International Society of Automation (ISA), these standards establish the requirements that are to be satisfied by key stakeholders in the area, namely the CII operators. Adopting and enforcing these standards could potentially serve as adequate guidelines that the operators can use in ensuring the CIIP. Obviously, the mandated institution may likewise consider adopting standards of the regional organizations like the ETSI; however, they have to suit Azerbaijan's current CIIP needs.

In this case, one may also look at the Turkish experience to see how they have standardized their cybersecurity operations. In comparison to the standardization of its military assets, which follow the NATO standards, Türkiye has applied the general ISO/IEC 27001 standards for ensuring its data security; nevertheless, it is also following certain sectoral standards established by the Information and Communication Technologies Authority (ICTA), which is a national regulatory and inspection authority of the country (Kasap & Sönmez, 2020). What is interesting to note is that Türkiye has so far been relying on its domestic capacities to develop the necessary standardization, meaning it has not looked for alternatives elsewhere. According to Kasap & Sönmez (2020), the ICTA helps develop the needed cybersecurity standards by convening meetings with cybersecurity professionals and gaining their input to determine the standards and procedures. However, in 2016, Türkiye also received the EU assistance in helping the country align its cybersecurity policies with that of its NIS Directive. Following that, on February 5, 2020, the ICTA hosted the closing event of the project of the implementation of the NIS Directive in Türkiye, as a result of which the country managed to develop its cybersecurity legislation and methods (e-Governance Academy, 2020). Considering this and the fact that Türkiye is not a member of the EU, it is possible and advisable for the Government of Azerbaijan to pursue a similar policy, especially considering that the NIS-2 Directive has come into existence. Furthermore, the Turkish Cyber Security Cluster, supported by the Digital Transformation Office under the Presidency of the Republic of Türkiye, serves as a platform that allows for the development of the country's cybersecurity ecosystem and identifying its evolving needs. Given its purpose, the representatives of different public institutions, private companies, and academia use this platform to determine the evolving needs in cybersecurity. Although there is already a commission on information security in Azerbaijan, the Government of Azerbaijan could also consider incorporating actors from the private sector and academia to come up with new standards and further enhance public-private partnership as a result.

3.2 Creating a Register for the Country's CII Assets and Classifying Them Based on the Factor of Criticality

Before proceeding any further with increasing the country's CIIP, it is highly advisable to identify all the CII assets operating in Azerbaijan and rank them ordinally based on the factor of criticality. To this end, the Government of Azerbaijan must consider creating a single register where it should feature all CII assets in the country and determine methods to be used for identifying the thresholds of their criticality. To do so, the government must first identify the existing CII in Azerbaijan and classify them according to the criticality factor. The significance of this course of action can be understood in the context of the option 3.3 (organizing activities on CIIP), which pertains to the establishment of ways of carrying out and monitoring activities on CIIP. In other words, in order for Azerbaijan to create an effective framework of activities in the area, it must first determine its priorities by carefully assessing the CII landscape. Mattioli & Levy-Bencheton (2014) state that this sort of assessment necessitates an active collaboration between the mandated agencies and operators of the CII and that the factor of criticality can be determined by considering their business value, the scope of population that use their services, and the degree of their dependence. There are obviously different ways through which countries identify the CII criticality; however, one particular way of doing this is by considering the potential impact that the disruption of their services can inflict on the functions of society and country as a whole.

Perhaps the most important development that has been in made in the EU in this area concerns the CER Directive which came into force on January 16, 2023. Replacing the Council Directive 2008/114/EC on the identification and designation of European CI and assessment of the need to improve their protection, the current directive is applicable to 11 sectors and requires the EU member states to adopt the necessary strategies to identify entities that are deemed critical or of vital importance to society (One Trust Data Guidance, 2023). Since the task of identification is left to the member states, it is curious to see how certain states do this. For instance, in the case of Germany, the Federal Ministry of the Interior (2009) devised a National Strategy for Critical Infrastructure Protection, in which it argues that "infrastructure is deemed critical whenever it is of great importance to the functioning of modern societies and any failure or degradation in the area would result in sustained disruptions in the overall system." As an example, the ministry provides an example of electricity and information and telecommunication infrastructures, the disruption of which can jeopardize public safety. In Russia, for instance, the government decree dated February 8, 2018, identifies criticality of CII assets based on three categories (I, II, and III), which are determined by 14 types of negative consequences that disruptions in their services can bring about (rulaws.ru, 2018). In the United States, the Cybersecurity & Infrastructure Security Agency (CISA) similarly defines CII as being composed of assets whose incapacitation can have debilitating effects on many sectors of the country.

Why should it matter for the Azerbaijani government to create a register and determine the criticality of the CII? For one, creating a register of CII will allow the government to organize activities of the mandated institutions and CII operators, while at the same time monitoring the maintenance of CIIP. At the same time, determining the criticality of such infrastructures will allow the government to make valid assessments, which will in turn allow for an effective distribution of resources to the development of critical infrastructures. This may be prevented in case the government overestimates the criticality of one asset. Another problem may arise if the government underestimates the criticality of an asset and thus render an organization susceptible to potential loss of services (KPMG, 2022). Therefore, in general, a disruption in services of one CII asset may not be of the same magnitude as the one of the other one, which is why it is essential that the government neither underestimates, nor overestimates the criticality factor. With that in mind, the government must begin incorporating CII assets into a single register and classifying them based on the approach that Mattioli & Levy-Bencheton (2014) coin as a "critical service-dependent approach." One of the versions of this approach is to have mandated state institutions prepare the list of all CII assets and operators to identify appropriate measures needed for maintaining their security. Following this course of action, the government may also consider categorizing CII assets based on more specific threshold such as ones employed by the Government of Russia.

3.3 Preparing a Blueprint for the System of Managing and Monitoring the CII Security

As previously mentioned, the mandated institutions and CII operators require guidance on how to establish an effective system for managing the country's CIIP. Therefore, in the meantime, the government must consider sketching at least the preliminary model of a management system that will outline the tasks and duties of all the relevant actors (i.e. the CII operators and mandated institutions), determine their relationship, while at the same time facilitating the exchange of information among them. In this sense, the development of such a model will help the government organize the usual processes in a manner that precludes potential risks, as well as establish a clear picture of what is expected from the relevant actors in the area. An essential part of this management system will be comprised of the functions of the mandated institutions.

Apart from what has already been said about the EU's CER Directive, especially how it compels the member states to determine the institutions in charge of the CIIP, one can refer to the German experience in establishing the necessary management system. Since its establishment in 1991, the Federal Cyber Security Authority (BSI) has been functioning as one of the key institutions with a competency of monitoring and auditing the developments in cybersecurity (bsi.bund.de, 2021). Its role as a federal cybersecurity authority was further expanded upon the signing of the Germany IT Security Act 2.0 that came into force in 2021. According to the country's latest national strategy of 2021, the CII operators in Germany are supposed to inform the BSI about the measures they take to ensure their security by submitting evidence on a regular basis. The BSI, on the other hand, carries out on-site checks, identifies the best technology to be implemented, and to this day continues assessing the criticality of the existing infrastructures, which is to suggest that it is an ongoing process (BSI, 2021). At the same time, in the current context, there is a network of state and federal institutions created by critical infrastructure protection offices and working groups, which helps the government take on a consolidated approach to the problem.

When it comes to Russia, however, Pursiainen (2021) argues that the Federal Security Service (FSS) practices the leading role in the country's CIIP, while also maintaining that the existing legislation holds the CII operators to be legally responsible for registering and taking care of their own infrastructure. More importantly, the 2017 federal law delegates the task of determining the criticality of CII assets to operators. Additionally, the CII operators must submit upon the request of the executive bodies the required information on their activities, as well as comply with their requirements. In the United States, the latest change came with the enactment of the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) which requires that CII operators report on cyber incidents and ransomware payments to the CISA so as to enable the latter to render the necessary assistance (CISA, 2022).

In the previous section, it was established that the State Security Service and the State Service for Special Communication and Information Security have been recognized as the institutions in charge of managing the Azerbaijani CIIP. Drawing on what has previously been said, the Government of Azerbaijan must now create a setup that will allow the mandated institutions and CII operators to carry out a collaborative work. Specifically, the CIIP management system must create obligations for the CII operators to ensure that the information systems used in the daily operations of the infrastructure remain operational, as well as minimize the potential risks that may be posed by cyber incidents in accordance with the predetermined standards. The guidelines of such a system are to be based on the establishment of general CIIP requirements and the characteristics (e.g. standard operating procedures) of the CII operators. In this regard, the CII operators must at all times report to the mandated institutions on all cyber incidents and measures that are taken to mitigate the risks. In order to realize these elements of the CIIP management system in Azerbaijan and maintain its effective operation, the mandated institutions must at all times monitor the overall situation in the CIIP; coordinate the implementation of joint measures needed for thwarting potential cyber threats; analyze the existing gaps in the CIIP, be it on a local or global scale, in order to discover vulnerabilities; advise the CII operators on the existence of such vulnerabilities by recommending measures regarding the elimination of malicious software and other sources of threats; and aggregate information on the CII incidents experienced by the operators.

Referring back to the Russian practice, one can see how the proposed policy option has already been put to test in the real world. In accordance with the Russian legislation (i.e. the Federal Law of 26 July 2017), the government has already created such a system that ensures complete control over the management of the CIIP and the work of all the relevant institutions. According to Pursiainen (2021), the Presidential order of 2013 made it clear that the FSS was to take the leading role in managing the country's CIIP system. As mentioned above, the system functions in a way that endows the FSS with overall control over its operations, while ensuring that the CII operators follow the prescribed standards. Here, it is worth mentioning that the CIIP management system operates through the criticality factor, which is suggested in the option above. In the case of Azerbaijan, the mandated institutions in charge of the CIIP have already been identified; however, it is important to establish how the management system will work.

3.4 Promoting Research and Development in Cybersecurity

Aside from establishing the much-needed system for managing the CIIP in Azerbaijan, coupled creating ordinance of the CII assess and basic requirements, it is also advisable for the government to think of the long-term development of the area, which is to be achieved by increasing research and development in the field. In addition to raising general awareness on what cybersecurity entails, it is also necessary for Azerbaijan to bolster the domestic R&D in cybersecurity in order to be able to devise its own solutions for the CIIP. For instance, during the seminar organized by the AKTA (6 April 2023), the representatives of the mandated institutions, as well as other cybersecurity organizations, broached upon the matter of software usage. Because most, roughly 81% as reported by the Software Alliance (2018), of the used software is pirated, the institutions are planning to promote the local production of software that can be certified. During the discussions, the participants agreed on one point: in order for the government to achieve this, it needs to stimulate R&D in cybersecurity.

In this case, one can again consider the state of R&D in the EU. As Di Franco (2018) argues, the EU has the necessary capacity to bolster the bloc's R&D in cybersecurity. As an example, the author brings up the "Horizon 2020" which was the EU's funding programme for research and innovation that lasted from 2014 to 2020. There is also Digital Europe Programme that focuses on upscaling digital capacity of the EU member states while also focusing on bolstering their cyber defense capabilities. While the focus of these programmes goes beyond cybersecurity to include a wide range of innovative solutions, Di Franco (2018) claims that projects need not be completely based on cybersecurity and that matters related to cybersecurity constitute an important part of the European R&D.

However, perhaps an even more noteworthy example of the European R&D concerns the establishment of the European Cybersecurity Competence Centre (ECCC), the purpose of which is to promote technological capacities of the member states by gathering resources from the EU and making shrewd investments. On the other hand, it also helps to analyze the state of cybersecurity R&D in the United States. The so-called Cybersecurity Enhancement Act of 2014 requires that the National Science and Technology Council and the Networking and Information Technology Research and Development Program develop and update the country's strategic plan for promoting R&D in cybersecurity (Cyber Security and Information Assurance Interagency Working Group, 2019). Every four years, the strategic plan is updated to establish the new priorities, as well as identify the roles of the relevant institutions. The strategic plan of 2019 identifies artificial intelligence, quantum information science, trustworthy distributed digital infrastructure, privacy, secure hardware and software, and education and workforce development; however, it is important to note that the priorities change over time. Overall, however, the authors of the plan (2019) argue that strategic government investment in cybersecurity R&D can give additional impetus to the country's capacity by helping it counteract adversary's asymmetrical advantage in cyber space.

In this regard, and considering all of the above, the policy option advises that Azerbaijan considers promoting R&D by making strategic investments in promising initiatives, especially ones concerning CIIP. In reference to the previous point, there is an unfair degree of asymmetry in cyberspace, which is suggestive of the observation that governments must always keep coming up with new solutions to constantly emerging threats. Developing legislation, creating ordinance of the CII assets, and establishing the model for managing CIIP are all important; nevertheless, the only way to truly bolster Azerbaijan's capacity in the area on a long-term basis is through effective R&D measures. A possible starting point for stimulating development in this area could be through the "Cyber Security Center" established by the MDDT and Pasha

Holding. In this context, it is also advisable that the government follows adopts a practice similar to the one of the US. That is, it may consider adopting the equivalent of the R&D strategic plan in order to give force to the local R&D endeavors.

3.5 Incorporating Courses on Cybersecurity into Tertiary Education Curricula

The safeguarding of critical information infrastructure (CII) is an essential component of both national security and public safety (ENISA, 2015). Cybersecurity incidents targeting the CII are capable of producing severe outcomes, such as substantial financial losses, fatalities, and interruption of vital utilities (ENISA, 2015). One viable strategy for mitigating this problem is to increase the level of public awareness regarding the safeguarding of the CII. In other words, an effective strategy that could be opted for today could be the integration of cybersecurity courses into the higher education curriculum, in order to increase cybersecurity awareness amongst the IT professionals and society in general.

Incorporating certain courses into the higher education curricula could prove beneficial for upscaling Azerbaijan's cybersecurity capacity, which is why the government should consider this option carefully (ereforms.gov.az, 2021). Using this technique, the government will ensure that the public can grasp the basic concepts and follow precautionary procedures both during the casual internet browsing and in times of emergency. Educating the younger generations and prospective students will ensure the development of the country's cybersecurity potential, which will in turn protect the country's CII from potential cyberattacks (Kertysova et al., 2018). To this end, it is advisable that students at higher education institutions enroll in several relevant courses featured in their syllabi. There could also be an option of educating or tutoring the staff of schools, universities, and other educational institutes, to develop a certain class in teaching their students with their methods in order for a better comprehension.

The EU, Russia, and the US have all undertaken certain measures to raise public awareness on safeguarding of the CII (Kertysova et al., 2018). The EU mandates through its NIS Directive that all member states must confirm that operators of essential services and digital service providers take adequate measures to mitigate the risks posed to their networks and information systems. The aforementioned directive mandates member states to guarantee that their populace is cognizant of the potential hazards that cyber threats pose and educate them on precautionary measures that can be implemented to safeguard themselves.

In accordance with the Federal Law on the Security of Critical Information Infrastructure in the Russian Federation, operators of critical information infrastructure are mandated to implement measures aimed at safeguarding their systems from cyber threats (CISA, 2022). It is requisite as per existing legislation to formulate a comprehensive national framework aimed at safeguarding critical information infrastructure (CII), in addition to constituting a dedicated commission tasked with the responsibility of ensuring the realization of such a strategy. Furthermore, the Russian government has undertaken several initiatives aimed at promoting the dissemination of knowledge amongst its populace regarding the critical significance of cybersecurity (CISA, 2022). Russia has instituted diverse measures aimed at heightening awareness concerning the regulation of critical information infrastructure. In 2018, the legislative body of the Russian Federation implemented a regulatory mandate stipulating that companies must maintain all personally identifying information pertaining to Russian citizens within the confines of the nation's geographic boundaries. The aforementioned legislation has faced disapproval for its potential to impede the availability of data and curtail the exercise of free expression (CISA, 2022). Moreover, the government of Russia has instituted the National Coordination Center for Computer Incidents, tasked with the responsibility of supervising and addressing cyber threats. The aforementioned center proffers instruction and direction to institutions in order to enhance their cybersecurity measures. Furthermore, Russia has demonstrated an active engagement in advancing collaborative efforts pertaining to the sphere of cybersecurity at a global level.

The Department of Homeland Security (DHS) in the US has implemented several measures aimed at enhancing public understanding of cybersecurity, one of which is the Stop.Think.Connect campaign (DHS, 2021). The aim of the following discourse is to present a revised and more academic version of the term "campaign". The campaign endeavors to provide guidance to American citizens regarding the potential dangers instigated by cyber threats and the proactive measures that they may adopt to ensure their safeguarding. Moreover, DHS has endeavored to provide a multitude of educational materials to assist instructors with integrating the subject of cybersecurity into their pedagogical plans (DHS, 2021).

Although efforts have been made by the EU, Russia, and the US to enhance public awareness regarding the CIIP, distinct disparities exist in the approaches adopted by these respective regions (European Commission, 2013). One illustration of divergent approaches to safeguarding critical information infrastructure can be observed in the contrasting foci of the EU's NIS Directive versus Russia's Federal Law on the Security of Critical Information Infrastructure (ENISA, 2015). The former prioritizes the protection of essential services and digital service providers, while the latter extends its reach to encompass a wider range of industries and sectors. Moreover, the United States has prioritized public awareness campaigns in combating the issue at hand, whereas the EU and Russia have adopted a more regulatory approach.

The EU has undertaken various measures to facilitate the integration of cybersecurity studies into the higher education curriculum, with the aim of urging member countries to establish cybersecurity programs (ENISA, 2015). The European Commission has initiated various programs aimed at promoting the advancement of cybersecurity competencies, which entail the establishment of a European Cybersecurity Skills Framework. Furthermore, the EU has inaugurated the European Cybersecurity Industrial, Technology and Research (ENISA, 2015). The EU has undertaken diverse initiatives aimed at enhancing consciousness regarding the regulation of vital information infrastructure. In 2016, the EU enacted the NIS Directive which outlines specific security and reporting obligations for critical service operators and providers of digital services. The EU has established the European Union Agency for Cybersecurity (ENISA), a specialized body that offers consultations and assistance to its member states regarding cybersecurity concerns. As such, the ENISA assumes responsibility for overseeing the management of the CERTs across member states. The EU has demonstrated an active role in advancing international collaboration in matters concerning cybersecurity and has instituted collaborative partnerships with other countries and entities with the aim of enhancing cybersecurity on a global level.

Chapter 4. Evaluation of the Policy Alternatives

The following chapter features the evaluation of the policy alternatives enumerated in the previous section. The evaluation will be done along five standard criteria, namely effectiveness, efficiency, equity, feasibility, and flexibility. Following the evaluation, three policies – two primary and one secondary – options will be chosen, and the rationale for the choices will be provided.

Adopting CII Standards in Azerbaijan

The previous chapter touched upon the importance of valid standardization in ensuring the effective maintenance of the CIIP. The option of adopting CII standards and enforcing them on a national level is by all means effective, as such standards will allow the CII operators to base their operations on proper practices and pave the way for service optimization. It can be surmised from the personal communication with the representatives from the MDDT and other relevant institutions that it is near to impossible to build an effective CIIP scheme without the use of effective standardization. In this regard, the option is effective, as it suggests an inevitable course of action. Furthermore, one can argue that the option is efficient, in the sense that its implications for the CIIP are efficient. Valid CII standards, if adopted, will guide the operators in choosing the most optimal options and technologies, thereby minimizing the possibility of proceeding with ineffective choices (from personal communication with LK from the MDDT, 28 April 2023). As for equity, it is safe to assume that the current option satisfies the criterion. Given the significance of standardization and the benefits that it is to yield to the CIIP, one can go on to argue that benefits do in fact outweigh costs. The only potential cost may manifest in the inability or reluctance of the CII operators to adapt their operations to the new standards; however, with proper enforcement mechanisms, this challenge is only temporary. Is the option feasible? It surely is. To reiterate, the option does not advocate creation of standards from nothing; rather, it argues for adoption of appropriate international standards that have already proven to be effective. Obviously, adoption of such standards entails that the government goes through some requisite procedures. However, it is feasible, as Azerbaijan has already developed 59 general cybersecurity standards based on the international ones. When it comes to flexibility, that is where the option may fall short of satisfying all criteria. This option concerns adoption of rigid, albeit effective, standards that are not to be swayed left and right. Again, although some operators may find it difficult to accustom themselves to the standards, they may not derogate from them.

Creating a Register of the Country’s CII Assets and Arranging Them Based on the Factor of Criticality

In addition to the adoption of effective standards, ensuring the CIIP in Azerbaijan also requires that the mandated institutions have a clear understanding of the country's CII landscape. For this, the option proposes that the institutions create a single register of CII assets and create a hierarchical order based on their criticality. In terms of effectiveness, the evidence shows that most mandated institutions such as the Federal Ministry of the Interior in Germany, the CISA in the US, and FSS in Russia emphasize the importance of criticality. Therefore, creating a register of CII assets akin to the one of the Department of Home Affairs in Australia will allow the government to understand the arrangements of the assets, which will enable it to correctly assess their criticality and risk factors that come with them. Therefore, it is effective. Is it an efficient option? The creation of such a register may incur a considerable setup cost; however, its implementation will ultimately yield greater benefits. That is, the register will, inter alia, allow the government to eliminate unnecessary losses in finances, time, and effort in attempt of creating individual approaches to the CIIP. That is because the classification that comes with the register will allow it to build a consolidated approach to the CIIP, meaning it will prove efficient. The option satisfies the equity criterion, following that there is a fair distribution of costs and benefits. In reference to the previous point, the creation and classification of the CII assets will inevitable incur considerable financial costs. However, in light of all of its benefits to the CIIP maintenance, the trade is off more than fair. When it comes to determining the feasibility of the option, the evidence, again, suggests that it is possible to develop and operate a fully-functioning CII assets register. The best example in this case is the CII register that was developed by the mandated institution in Australia. Of course, creating such a system requires the government to go through a series of procedures; however, creating a registry is definitely feasible and advisable. Lastly, the option is to a certain degree flexible, in the sense that there are no rigid requirements for creating the register. It goes without saying that the register's work after development should remain true to its purpose; nevertheless, when establishing the system, there is no reason for the government not to incorporate feedback from all the involved institutions. In this regard, it would seem that this option also satisfies all criteria.

Preparing a Blueprint for the System of Managing and Monitoring the CII Security

The option of preparing a blueprint for a system of managing and monitoring the CIIP is definitely effective, in the sense that it proposes establishment of mechanisms that will have to be created at some point. What is meant by system in this case is essentially the state of relationship between the mandated institutions and the CII operators, regulations guiding their conduct, as well as legislation identifying their roles vis-à-vis one another. In this regard, the option is effective. As for efficiency, this depends on whether the option is to focus on short or long term development. In case of the latter, laying the ground for such an institutional setting will definitely incur financial costs; however, all costs are to be outweighed by potential benefits that are to be generated. This may not necessarily be the case in the short term, as devising such a management system may take considerable time and therefore be inefficient. However, considering that the current project focuses on the immediate deliverables, the option is deemed as inefficient. When it comes to equity, the policy satisfies the criterion, as it entails a fair trade off. Granted, one can very well expect there to be financial costs, but all of this is to establish a CIIP management system that will be guiding all the processes in the area for years to come. Is this feasible? The experience of countries like Germany, the United States, and Russia show that it is in fact feasible. Nonetheless, this again depends on whether it is a short or long term development. That said, creating this system requires time, which is why it is not feasible in the current context. Finally, when it comes to flexibility, the option does satisfy the criteria. The fact that many countries have managed to establish effective management systems shows that it is possible; however, it does not mean that their practice is uniform. That said, creating such a CIIP management system in Azerbaijan is flexible, as the government will have to take into account varying interests and ultimately factor them in when creating the model. All in all, it would seem that the option falls short of satisfying two criteria, namely efficiency and feasibility.

Incorporating Courses on Cybersecurity into Tertiary Education Curricula

The following option is effective, as it envisages the development of the needed mindset in youth. In other words, developing the institutional setting for maintaining the CIIP will not suffice, as it is also essential that the government develops potential cadres and responsible users. In the previous section, it was highlighted that phishing attacks constitute the biggest portion of all cyber-attacks in Azerbaijan. Given that its effectiveness depends on users, it is crucial that the government provides the necessary training and courses on cybersecurity for both graduate and undergraduate students and inform them of basic principles of cybersecurity and CIIP. The latter is perhaps even more important, considering that social hacking targeting humans can also pose similar threats to the CIIP. Is this efficient? Most definitely. Granted, the government will have to finance the creation and incorporation of such courses in tertiary education, but the impact that is to bring out far outweighs costs. By endowing citizens with a general understanding of what constitute cyber threats, the government will essentially pave the way for the recruitment of well-informed cadres in the CIIP, as well as the creation of a responsible mindset among users. The option likewise satisfies equity criterion, as the associated costs justify the ends. Coming to feasibility, the current option most certainly satisfies the criterion, as there are numerous institutions providing cybersecurity courses at educational facilities. Whether it is possible in the short term, however, is up to a question. Normally, if one was dealing with a country that ranked low on most of the reputable cybersecurity indexes, it would not be realistic. However, there are currently several organizations like STEP IT Academy that have already developed certain programmes. Still, there may not be sufficient experts on the CIIP, which is why creating such programmes in short time may prove unfeasible. Nevertheless, the option is flexible, in the sense that cybersecurity can include a large variety of capacity-building courses. Although there may not be enough experts specializing in the CIIP, the actors may devise courses that can temporarily compensate for the lack of courses in that very area.

Promoting Research and Development in Cybersecurity

This option definitely satisfies the effectiveness criterion, as it is all about building up the country’s cybersecurity capacity through continuous R&D. The findings demonstrate that most of the leading actors in cybersecurity such as the EU and the US place a great importance on funding and supporting potential initiatives in the area. In this sense, pushing the idea of promoting R&D in Azerbaijan equates to building a backbone to the CIIP development on a long-term basis. Whether the option is efficient or not is debatable. As of now, there is a cybersecurity center that serves as one of the few, if not only, R&D institutions in Azerbaijan. That said, promoting R&D may not yield the anticipated results, as there is a considerable lack of cybersecurity specialists in the country. Because promoting R&D requires great financial resources, the option may not be efficient in short term. As for equity, the question is again up for a debate. Financing R&D initiatives, be it through creation of special facilities or programmes, may not yield immediate benefits, as there is a lack of cybersecurity specialists. However, the option is definitely feasible. The experiences of the EU and the US prove that

R&D in cybersecurity can be effective if supported correctly. In case of the former, there are a number of ongoing programmes and projects, all of which catalyze R&D in the area. This option also has a fair degree of flexibility, as R&D can encompass various areas of relevance to the field. As such, it can be molded into any shape for as long as it translates into effective domestic solutions.

Evaluation Summary

Policy alt. & Criteria	Effectiveness	Efficiency	Equity	Feasibility	Flexibility
Adopting CII Standards in Azerbaijan	+	+	+	+	
Creating a Register of the Country's CII Assets and Arranging Them Based on the Factor of Criticality	+	+	+	+	+
Preparing a Blueprint for the System of	+			+	+

Managing and Monitoring the CII Security					
Incorporating Courses on Cybersecurity (CII) into Tertiary Education Curricula	+	+	+	+	+
Promoting Research and Development in Cybersecurity	+			+	+

Chapter 5. Policy Recommendations and Conclusion

As far as the paper is concerned, all of the presented options are of great significance to the development of Azerbaijan’s capacity in the CIIP. However, there are a few priority policies that call for the government’s consideration. It thus follows that the implementation of these policies may later create a different and more consolidated set of policies.

While awaiting the adoption of the national cybersecurity strategy, the mandated institutions must begin works on developing an exhaustive list (register) of the CII assets in Azerbaijan and preparing the preliminary model of the register that is to contain the information. Not only that but the institutions must also determine criticality of such assets, according to which they latter will be arranged in hierarchical order. The logic here is to develop a sufficient understanding of the current CII landscape so as to make an effective transition to the provisions of the national cybersecurity strategy.

At the same time, the government must also consider adopting a set of valid international standards for the CIIP, as they are absolutely necessary for ensuring the proper organization of the CII assets and conduct of their operators. The evaluation has shown that adopting rather than developing such standards is highly effective and reliable, which is why it is advisable that the government adopts them as early as possible. Doing so will aid in streamlining processes later on.

The last option that the government should take into account is related to providing students at higher educational institutions with cybersecurity (CII) courses. This option, coupled with the preceding two, will allow the government to maximize its capacity in maintaining CIIP, as it also entails the development of potential cybersecurity cadres in Azerbaijan. It is even to plausible to assume that this option will go hand in hand with the others, as the sustainability of the country's capacity development in cybersecurity comes down to its people.

Concluding Remarks

The main goal behind the present Capstone project is to provide the Government of Azerbaijan, specifically the mandated institutions, with various policy options that can catalyze the country's CIIP following the adoption of the national strategy. In addition to analyzing the current situation in the country, the capstone project also looks into the practices of different countries, mainly from the EU, to see how and what options can be proposed for implementation in Azerbaijan.

Although Azerbaijan has a potential to maximize its cybersecurity capacity and ensure the CIIP, the findings show that more needs to be done in terms of raising public awareness on cybersecurity, developing cybersecurity cadres, and promoting R&D in this particular field. These areas essential, as they constitute and will remain priority areas for years to come.

Given that the global practice, as illustrated through a comparative analysis of the EU member states practices, the current capstone paper proposes a few options that can prove beneficial to the ensuing processes. These options are options entailed a) adoption of certain CII standards b) creation of a single register of the CII assets in Azerbaijan c) preparing the preliminary blueprint for the CIIP management system in Azerbaijan, as well as d) incorporation of cybersecurity courses focusing into curriculum and e) and promotion of Research and Development in cybersecurity. The rationale is to provide the government with some options that are advisable to pursue in the current context, as they reflect the global practice and have proven to work in several cases (e.g. Germany and Russia).

Bibliography

Aghjayev, S. (2022). Main Types of Cyber Attacks in Azerbaijan Unveiled. Trend News Agency.

Alcaraz, C. & Zeadally, S. (2015). Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. International Journal of Critical Infrastructure Protection

Alcaraz, C. & Zeadally, S. (2015). Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. International Journal of Critical Infrastructure Protection.

Bruce. A. R. (2022). Cyber Security During International Conflict. Harvard Model Congress Boston 2022.

Confederation of the European Security Services (2022). CER Directive: EU law introduces quality control of security services in Critical Infrastructure Protection.

CISA (2022). Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure.

Decree no. 1315 of the President of the Republic of Azerbaijan (April 17, 2021).

Department of Homeland Security (2021). Stop.Think.Connect.

Di Franco, F. (2018). Analysis of the European R&D Priorities in Cybersecurity: Strategic Priorities in Cybersecurity for a Safer Europe. European Union Agency for Network and Information Security.

European Economic and Social Committee (2018). Opinion of the European Economic and Social Committee on ‘The cybersecurity challenge: How to enhance Europe’s resilience in the digital age.’ *Official Journal of the European Union*, C 440, 1-7.

ENISA (20215). Critical Information Infrastructures Protection Approaches in the EU.

Federal Ministry of the Interior (2009). National Strategy for Critical Infrastructure Protection (CIP Strategy)

Federal Ministry of the Interior, Building and Community (2021). Cyber Security Strategy for Germany 2021.

Ghernouti-Helie, S. (2010). A National Strategy for an Effective Cybersecurity Approach and Culture. 2010 International Conference on Availability, Reliability, and Security.

Gorniak, S. & Atoui, R. & Fernandez, J. & Quemard, J. & Schaffer, M. (2019). Standardization in Support of the Cybersecurity Certification. European Union Agency for Network and Information Security.

International Information System Security Certification Consortium (2022). Cybersecurity Workforce Study 2022.

International Information System Security Certification Consortium (2022). Cybersecurity Workforce Study 2022.

International Telecommunication Union (2021). Guide to Developing a National Cybersecurity Strategy. Strategic Engagement in Cybersecurity..

Ismayilova, N. (2020). Rauf Jabbarov: Training Personnel in the Field of Cyber Security is an Important Task. Trend News Agency.

Kasap & Sönmez (2020). Cybersecurity in Turkey. *Paksoy*.

Klynveld Peat Marwick Goerdeler (2022). Critical Infrastructure: Understanding Asset Criticality.

Markopolou, D. & Papakonstantinou (2021). The Regulatory Framework for the Protection of Critical Infrastructures Against Cyber Threats: Identifying Shortcomings and Addressing Future Challenges: the Case of the Health Sector in Particular, Computer Law and Security Review.

Mattioli, R. & Levy-Bencheton, C. (2014). Methodologies for the Identification of Critical Information Infrastructure Assets and Services. European Union Agency for Network and Information Security.

Mavroeidis, V. (2017). Cybersecurity education in higher education: A study of the current state of and future prospects for cybersecurity programs in post-secondary education. *Journal of Education for Business, 92*(4), pp. 183-189

Mercer, W. (2020). PoetRAT: Malware Targeting Public and Private Sector in Azerbaijan Evolves. Talos Intelligence Blog.

Networking and Information Technology Research and Development (2019). Federal Cybersecurity Research and Development Strategic Plan.

One Trust Data Guidance (2023). EU: CER and NIS 2 Directives Enter Into Force.

Personal Communication with the Representative of the Ministry of Digital Development and Transport (3 April 2023).

Pursiainen, C. (2020). Russia’s Critical Infrastructure Policy: What Do We Know About It? European Journal for Security Research. 6, 21-28.

Resilience and CIIP. (n.d.).

Resolution no. 127 of the Government of the Russian Federation (February 8, 2018).

Scarfone, K. & Benigni, D. & Grance, T. (2010). Cyber Security Standards. National Institute of Standards and Technology.

Security Week (2022). Nation-State Hacker Attacks on Critical Infrastructure Soar: Microsoft.

Spinu, N. (2020). Azerbaijan Cybersecurity Governance Assessment. Geneva Centre for Security Sector Governance.

Srinivas, J. & Das. A. K. & Kumar, N. (2019). Government Regulations in Cyber Security: Framework, Standards, and Recommendations. Future Generation Computer Systems, 98, pp. 1-13.

The NATO Science for Peace and Security Programme (2022). Azerbaijan: Developing Practical Cooperation through Science.

Vigdor, D. (2023). How Do We Close the Skills Gap in the Cybersecurity Industry? Forbes.

Wenger A. & Mauer, V. & Cavelty M.D. (2009). International CIIP Handbook 2008/2009. Center for Security Studies, ETH Zurich