Scientific and Practical Cyber Security Journal (SPCSJ) 8(4): 66 – 71 ISSN 2587-4667 Scientific Cyber Security Association (SCSA)

CYBERSECURITY IN AZERBAIJAN: LEGISLATIVE MEASURES TO PROTECT CRITICAL INFORMATION INFRASTRUCTURE

Dr Balajanov Elvin
Chairman of the Association of Cybersecurity Organizations of Azerbaijan
ebalajanov@akta.az

ABSTRACT: The scope of information infrastructures underpinning business operations and technological processes within Azerbaijan's national security sectors is rapidly expanding. These infrastructures are essential for ensuring operational continuity and resilience, with any compromise posing a risk of significant disruption and damage. Consequently, safeguarding these infrastructures has become a core priority within the nation's broader information security strategy. To this end, substantial measures, including enhanced legal regulations, have been implemented to strengthen the security of infrastructures deemed critical, as well as the information systems, communication networks, and automated management systems vital to the interests of the state, society, and its citizens. This article examines the legal frameworks established for the protection of critical information infrastructure (CII) in Azerbaijan, while also identifying areas needing further development and optimization.

KEYWORDS*:* critical information infrastructure, *CII, Azerbaijan, legal regulation, criticality criteria, security requirements, cybercrime, legal liability.*

INTRODUCTION

In the rapidly evolving global information space, states are consistently broadening their efforts to secure national information independence and sovereignty while reliably safeguarding their national interests. Consequently, a comprehensive set of measures in information security and cybersecurity is being implemented to address these challenges. In the Republic of Azerbaijan, where digital transformation is progressing rapidly, a robust information infrastructure is being established to address issues of society and state significance through information technologies. In particular, the scope of information infrastructures underpinning business functions and technological processes in critical sectors, including state and private entities as well as civil organizations, is expanding swiftly. Any compromise in the security of these infrastructures could lead to substantial harm, thereby making their protection a crucial component of the nation's core interests in the information sphere.

It should be particularly noted that ensuring the security of critical information infrastructure (CII) is one of the nine priority areas outlined in the *Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027* approved by the Decree of the President of the Republic of Azerbaijan No. 4060, dated August 28, 2023. The strategy emphasizes the critical importance of ensuring the information security of infrastructures that are pivotal in supporting the vital functions of society and the state, as any failure or disruption in their operation can have profound consequences on public health, safety, economic stability, social welfare, and the uninterrupted functioning of state institutions. Thus, the security of CII must remain a primary focus, regardless of its ownership, and appropriate measures must be implemented to safeguard it. (*Information Security and Cybersecurity Strategy* 2023, 6.4.)

Consequently, significant steps have been undertaken across various sectors in Azerbaijan, including legal regulation, to address issues essential to the state, society, and citizens and to enhance the security of CII, along with the associated information systems, communication networks, and automated management systems.

FACTORS CHARACTERIZING THE CRITICALITY OF INFORMATION INFRASTRUCTURE AND THE LEGAL MECHANISMS APPLIED FOR THIS PURPOSE

As outlined in the *Presidential Decree* of the Republic of Azerbaijan dated April 17, 2021, *"On Certain Measures for Ensuring the Security of Critical Information Infrastructure"*, the continuous development of information technologies and the globalization of information and information systems have become crucial tools for the country's progress. Thus, in the Republic of Azerbaijan, an appropriate information infrastructure is being developed to address matters of national importance, and its integration into global information networks, including the internet, has exposed infrastructure objects to cyberattacks. The disruption or malfunction of the systems and networks within CII, established to safeguard the rights and interests of the state, society, and citizens, can result in severe damage, which makes the cybersecurity of CII a priority issue (*the Presidential Decree "On Certain Measures for Ensuring the Security of Critical Information Infrastructure"* (2021).

It should be noted that the Law of the Republic of Azerbaijan No. 539-VIQD, dated May 27, 2022, introduced a new chapter titled "Security of Critical Information Infrastructure" and several related concepts to the *Law on "Information, Informatization, and the Protection of Information."* According to this law, CII encompasses a set of information systems, automated management systems, and information-communication networks that ensure the functioning of sectors such as public administration, defense, healthcare, financial markets, energy, transportation, information technology, telecommunications, water supply, and ecology, the disruption of whose functionality could cause significant harm to the state, society, and citizens' interests (*Law "On Information, Informatization, and the Protection of Information"* 1998, article 2) Thus, ten sectors have been identified in the Republic of Azerbaijan as having CII:

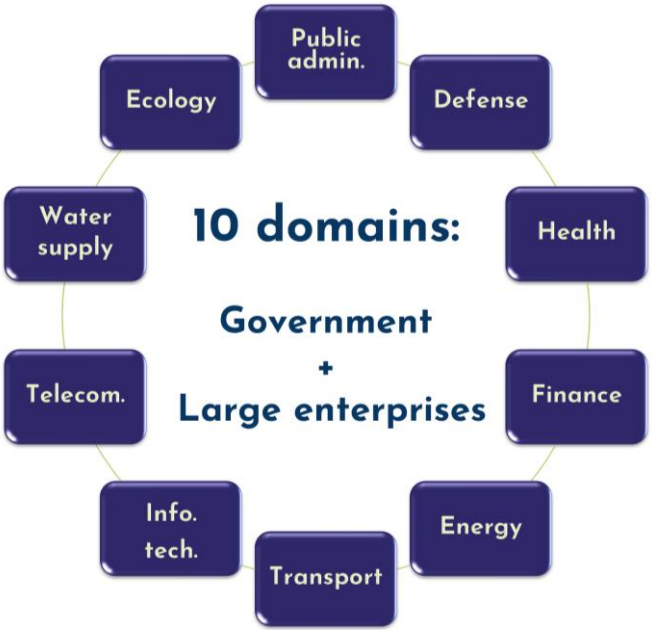

***Figure 1**. Critical Information Infrastructure Sectors in Azerbaijan*

According to the *Law on "Information, Informatization, and the Protection of Information"*, a CII object refers to an information system, automated management system, or information and communication network that is part of CII, while "a CII subject" refers to the state bodies (organizations) that own (or use) the CII object, including state-owned legal entities, public legal entities created on behalf of the state, as well as other legal entities and individual entrepreneurs (excluding micro, small, and medium-sized enterprises). (Ibid., article 2)

In both national and international practice, one of the most crucial and complex issues is determining the criteria for identifying CII objects. In the Republic of Azerbaijan, the list of CII objects is approved based on several requirements. According to the Law, an object is considered a CII object if its disruption could result in the following outcomes:

" - threats to the independence, sovereignty, constitutional order, territorial integrity, and defense capabilities of the state;
- significant threats to public safety;
- below situations leading to the deprivation of essential services for the population:
  - disruption of the functioning of state bodies (institutions);
  - serious obstacles to the normal functioning of life-supporting infrastructure;
  - interruption of transportation and communication links;
  - significant limitations on the provision of healthcare services;
- disruption of economic and financial stability;
- severe damage to the formation of the state budget;
- disruption of ecological balance and sharp deterioration of the environmental situation." (*Law on "Information, Informatization, and the Protection of Information" 1998, Article 20-2*)

Although the criteria set by the law are somewhat clear, the lack of definitions for descriptive terms such as "significant threats", "serious obstacles", "severe damage", and "sharp deterioration" could create difficulties in determining the scope of CII objects in practice. Specifically, the meaning of the "significance" of threats, the "severity" of damage and restrictions, and the "sharpness" of deterioration remains unclear.

SECURITY REQUIREMENTS FOR CII OBJECTS

In general, according to Article 20-1.1 of the Law, the security of CII is ensured through the establishment of security requirements for the infrastructure, the assessment of its compliance with these requirements, the elimination of identified non-compliance, the implementation of an information security management system corresponding to these requirements, and the monitoring of the security of CII. (Ibid., Article 20-1.1)

Furthermore, the Law stipulates that both general and specific requirements for the security of CII must be determined, taking into account its purpose and operational characteristics, and these requirements must be included in the registry of CII objects. (Ibid., Article 20-4)

It should be noted that the rules for ensuring the security of CII, including the general requirements for the security of CII and the requirements for cybersecurity service providers, their personnel, technological resources, and operational processes, are established by the *"Rules for Ensuring the Security of Critical Information Infrastructure in the Republic of Azerbaijan*", approved by the Cabinet of Ministers of the Republic of Azerbaijan on July 17, 2023, Decision No. 229. According to the Rules, CII entities must comply with 29 general requirements across 7 areas/objectives, as well as specific requirements:

Figure 2. *Security requirements for CII objects*

The "*Decree of the President of the Republic of Azerbaijan on the Implementation of the Law of the Republic of Azerbaijan on Information, Informatization, and Information Protection*" (1998) determines that the responsibility for ensuring the security of critical information infrastructure (excluding the information infrastructure of protected persons and protected objects), including combating cyber threats, lies with the State Security Service of the Republic of Azerbaijan. The State Security Service, along with the Special Communications and Information Security State Service of the Republic of Azerbaijan, carries out these functions with respect to government bodies, public legal entities created on behalf of the state, and state-owned legal entities. (Article 2.2-1) In turn, the CII subject ensures the security of its infrastructure in accordance with the established general and specific security requirements.

The competent authority and CII subjects are responsible for monitoring the security of critical information infrastructure, ensuring compliance with both general and specific security requirements. The competent authority should support CII subjects in safeguarding state and societal interests, while overseeing the overall security of CII. It is also specified that the oversight of the security of CII is carried out through the evaluation of compliance with general and specific requirements, the resolution of identified non-compliance, verification of adherence to these requirements, continuous (24/7) monitoring of the security of CII, conducting penetration tests, and performing external audit inspections.(*"Rules for Ensuring the Security of Critical Information Infrastructure in the Republic of Azerbaijan"* 2023, Article 9).

Additionally, it should be noted that the *"Regulations on the Structure, Creation, and Maintenance of the Registry of Critical Information Infrastructure Objects"* approved by the Cabinet of Ministers of the Republic of Azerbaijan on July 17, 2023, define the legal, organizational, and technological foundations for the creation and operation of the registry. According to these regulations, the registry is an information system intended for carrying out information processes related to CII objects (such as data creation, collection, processing, storage, retrieval, protection, and exchange), as well as for ensuring the security of CII, including planning and executing measures for combating cyber threats and conducting analyses. ("Regulations on the Structure, Creation, and Maintenance of the Registry of Critical Information Infrastructure Objects" 2023, Article 1.2). The operator of the registry is the Cybersecurity Operations Center of the State Security Service of the Republic of Azerbaijan. Regarding state institutions, the operator's functions are carried out in cooperation with the cyber center of the Special Communications and Information Security State Service of Azerbaijan. (Ibid, Article 1.4). The organization and functionality of the registry's operation are ensured based on the information submitted by CII subjects. The submission of data is done in line with the operator's methodological recommendations and provided templates. (Ibid, Articles 5.1-5.2).

LEGAL RESPONSIBILITY MEASURES IN THE FIELD OF CRITICAL INFORMATION INFRASTRUCTURE SECURITY

The legal responsibility measures for ensuring the security of CII seem to take a more reactive approach, rather than proactively and effectively addressing potential risks. While penalties for non-compliance or failure to report incidents are in place, these measures may not be stringent enough to prevent or minimize threats effectively.

According to Article 371-1.1 of the *Administrative Offenses Code of the Republic of Azerbaijan* (2015), in case of violation of general and specific requirements by the owner of the infrastructure, its officials, or the provider (supplier) providing cybersecurity services, the officials are fined between 500 and 1000 AZN, and legal entities are fined between 3000 and 4000 AZN.[1] As per Article 371-1.2 of the same Code, officials who violate requirements related to the creation and functionality of the information security management system are fined between 1000 and 1500 AZN, and legal entities are fined between 4000 and 5000 AZN. Additionally, if the subject fails to report cyberthreats, cyberattacks, cyber incidents, and attempts to commit these actions against CII objects to the relevant state authority, officials are fined between 300 and 500 AZN, and legal entities are fined between 500 and 1000 AZN.

[1] Note: 1 AZN = 0.55 EUR as of the time of writing this article.

Moreover, according to Article 602-3 of the Administrative Offenses Code, if an official or the relevant authority fails to comply with the requirement to eliminate violations of general and specific requirements, or fails to create the necessary conditions or obstructs the detection, prevention, and investigation of cyber threats, cyberattacks, and security incidents, officials are fined between 1000 and 1500 AZN, and legal entities are fined between 4000 and 5000 AZN.

Additionally, it should be noted that according to the *Criminal Code of the Republic of Azerbaijan*, illegal access to, illegal interference with, and the illegal acquisition of data concerning the computer system of a CII object ("publicly significant infrastructure object") lead to criminal liability. The perpetrators of these crimes can face imprisonment for a period of four to six years, along with disqualification from holding certain positions or engaging in specific activities for up to three years (*Criminal Code of the Republic of Azerbaijan* 1999, Articles 271-273). This implies that cybercrimes targeting critical information infrastructure (CII) objects are classified as "minor crimes" under the Criminal Code.[2]

In general, the classification of cybercrimes committed against critical information infrastructure — considered crucial for the state's, society's, and citizens' interests, and whose security breaches could result in severe damage — as "minor crimes" can be disputed. For similar actions, such as those in the United Kingdom, penalties of up to fourteen years of imprisonment and even life imprisonment are imposed. (see, *UK Computer Misuse Act 1990*, 3ZA) This raises questions about whether the penalty set in the United Kingdom's legislation is excessively severe. However, it can also be argued that the penalty established in the *Criminal Code of the Republic of Azerbaijan* is not entirely proportional to these criminal acts, and in some cases, may be considered lenient.

CONCLUSION

Significant steps have been taken in various fields, including legal regulation, to strengthen the security of CII and its components, such as information systems, communication networks, and automated control systems in Azerbaijan. These initiatives aim to address key concerns that affect the state, society, and citizens, ensuring greater protection of vital infrastructure and enhancing national security efforts.

Specifically, criteria for identifying CII objects have been established, and security requirements for these objects have been clearly defined. Moreover, legal mechanisms for ensuring the security of CII, including organizational measures and oversight of safety conditions, have been implemented.

Additionally, it would be valuable to clarify certain descriptive terms used in the relevant normative legal acts mentioned above. A reassessment of the adequacy of the legal responsibility measures outlined in the legislation concerning violations related to CII would also be beneficial to ensure that they align with the evolving nature of cyber threats and security challenges.

ACKNOWLEDGMENT

This work was supported by Shota Rustaveli National Science Foundation of Georgia (SRNSFG) - CG-24-220

REFERENCES:

Strategy of the Republic of Azerbaijan on Information Security and Cybersecurity for 2023–2027 (Approved by Decree No. 4060 of the President of the Republic of Azerbaijan, dated August 28, 2023).

Decree of the President of the Republic of Azerbaijan "On Certain Measures for Ensuring the Security of Critical Information Infrastructure" (Decree No. 1315, April 17, 2021).

Law of the Republic of Azerbaijan "On Information, Informatization, and Information Protection" (Law No. 460-IQ, April 3, 1998).

[2] Note: According to Article 15.3 of the Criminal Code of the Republic of Azerbaijan, offenses that are punishable by imprisonment for a term not exceeding seven years, whether committed intentionally or through negligence, are classified as minor crimes.

Decree of the President of the Republic of Azerbaijan "On the Implementation of the Law of the Republic of Azerbaijan on Information, Informatization, and Information Protection" (No. 729, 19 june 1998).
NIS2 Directive - Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022, on measures for ensuring a high common level of cybersecurity across the Union.
Decree of the President of the Republic of Azerbaijan "On the Implementation of the Law of the Republic of Azerbaijan on Information, Informatization, and the Protection of Information" (Decree No. 729, June 19, 1998).
"Rules on Ensuring the Security of Critical Information Infrastructure in the Republic of Azerbaijan" (approved by the Cabinet of Ministers of the Republic of Azerbaijan, Decree No. 229, July 17, 2023).
"Regulations on the Structure, Creation, and Maintenance of the Registry of Critical Information Infrastructure Objects" (approved by the Cabinet of Ministers of the Republic of Azerbaijan, Decree No. 230, July 17, 2023).
Administrative Offenses Code of the Republic of Azerbaijan (2015) (https://e-qanun.az/framework/46960).
Criminal Code of the Republic of Azerbaijan (1999) (https://e-qanun.az/framework/46947).
UK Computer Misuse Act 1990 (https://www.legislation.gov.uk/ukpga/1990/18/contents).