



Institute for Development  
of Freedom of Information

COUNTERPART  
INTERNATIONAL  
In partnership for  
results that last.



# CYBERSECURITY REFORM IN GEORGIA: EXISTING CHALLENGES, INTERNATIONAL PRACTICE AND RECOMMENDATIONS



TBILISI  
AUGUST, 2020



AUTHORS:

Mari Malvenishvili, Cybersecurity Policy Researcher

Nini Balarjishvili, Researcher, Institute for Development of Freedom of Information (IDFI)

EDITORS:

Levan Avalishvili

Teona Turashvili

REVIEWER:

Javier Ruiz Diaz, Policy and Advocacy Consultant,  
Counterpart International



**USAID**  
FROM THE AMERICAN PEOPLE



Institute for Development  
of Freedom of Information

COUNTERPART  
INTERNATIONAL  
In partnership for  
results that last.



The study was prepared by the Institute for Development of Freedom of Information (IDFI). The contents of the study are the responsibility of IDFI and do not reflect the position of Counterpart International, United States Agency for International Development (USAID), and U.S. government.

© **Cybersecurity Reform in Georgia: Existing Challenges, International Practice and Recommendations, 2020**

**All rights reserved. It is forbidden to reproduce the study for commercial purposes without the written permission of IDFI.**

# CONTENTS

<b>INTRODUCTION</b> .....	6
<b>CYBERSECURITY ARCHITECTURE OF GEORGIA</b> .....	8
Background of Information Security Reform .....	9
Key Elements of the Information Security Law Adopted in 2012 .....	9
Organizations Responsible for Information Security .....	10
Challenges Related to Information Security and Law Enforcement .....	13
<b>RISKS AND CHALLENGES RELATED TO THE AMENDMENTS TO THE LAW OF GEORGIA ON INFORMATION SECURITY</b> .....	16
Summary of the Proposed Changes .....	17
Problems related to Categorization of the Subjects of Critical Information Infrastructure .....	17
The Excessive Mandate of LEPL Operative-Technical Agency of the State Security Service according to the Draft Law .....	18
Compliance of the Proposed legislative Amendments with the requirements of the Association Agreement with the European Union .....	20
Lack of engagement	22
<b>CYBERSECURITY ARCHITECTURE: INTERNATIONAL EXPERIENCE</b> .....	23
Introduction .....	24
Budget and Priority .....	25
National Strategy .....	25
Institutional Framework .....	25
Defining Critical Infrastructure .....	26
Access and Monitoring .....	26
Classification of Incidents .....	27
Military Conflict .....	28
Protection of Personal Data .....	28
Auditing and Testing .....	28
Accountability and Transparency .....	29

**POLICY RECOMMENDATIONS** ..... 30

**ANNEX 1: CYBERSECURITY REGULATORY FRAMEWORKS: INTERNATIONAL PRACTICE** ..... 34

The United States ..... 35

The United Kingdom ..... 40

Estonia ..... 44

France ..... 47

Germany ..... 49

**ANNEX 2: THE EUROPEAN UNION'S CYBERSECURITY FRAMEWORK** ..... 52

The NIS Directive ..... 53

EU General Data Protection Regulation (GDPR) ..... 56



## INTRODUCTION

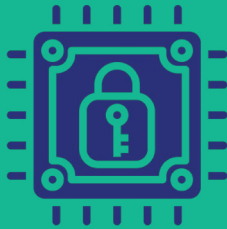
The growing importance of cybersecurity in the modern world security architecture makes it necessary to pay more attention to strengthening cybersecurity in Georgia. Georgia is a country that has repeatedly become the subject of cyberespionage and full-scale cyber-attacks. According to statistical data from the Ministry of Internal Affairs, the number of cybercrimes is increasing daily. Consequently, without an effective cybersecurity system, the stability and development of the country remains at risk. Given the fact that Georgia's existence and development have to contend with the tense geopolitical situation in the region, where non-state actors are becoming more active and cyberspace is used with increasing frequency for political purposes, Georgia may be at high risk of cyber-attacks.

Ignoring or inadequately assessing cyber threats will result in vulnerable economic structures, insufficiently protected critical infrastructure, and weakened overall capabilities, primarily in self-defense. Therefore, ensuring a high level of cybersecurity is vital.

This study shows that the measures taken by Georgia and the current cyber policy are insufficient to ensure cybersecurity and respond to modern challenges. As the country does not have strictly separated functions and responsibilities between state agencies, the mechanisms for coordination, cooperation, and information exchange have not been fully refined, a comprehensive list of critical infrastructure has not been developed, and the whole cyber system is not supported by proper legislative norms.

The study also demonstrates that a well-organized cyberspace architecture, properly distributed responsibilities, and mechanisms of accountability and coordination are key prerequisites for the effective and secure functioning of cyberspace.

Overcoming cyber threats, along with many other factors, depends on political will and proper management. Proper management, in turn, implies the proper redistribution of responsibilities and the refinement of coordination mechanisms. When a country is in a state of constant conflict and the risk of a massive cyber-attack is high, state resources should be mobilized to refine and strengthen the existing organizational system, especially given the fact that the current organizational system is designed with the direct involvement of strategic partners using best international practices. The current reality shows that the problem is in prioritizing cybersecurity as an important component of national security, rather than organizational rearrangement. Creating an effectively protected cyberspace requires a complex approach to the problem. To eliminate shortcomings, it is first and foremost essential to identify existing gaps and take appropriate measures to eliminate them.



## CYBERSECURITY ARCHITECTURE OF GEORGIA



## BACKGROUND OF INFORMATION SECURITY REFORM

Large-scale cyber-attacks carried out by the Russian Federation during the 2008 Russian-Georgian war, targeting government agencies as well as media outlets, severely damaged critical infrastructure in Georgia and made it clear that significant reforms were necessary for strengthening the information security system.

Precisely in 2008, with the support of Estonian experts, Georgia elaborated the so-called Roadmap and framework for its Cyber Security Strategy. **The Computer Emergency Response Team (CERT.GOV.GE)** was set up later in 2011. The main purpose of the CERT was the management of incidents against information security in the cyberspace of Georgia. At the same time, Georgian authorities started working on the **Law of Georgia on Information Security**, which entered into force in 2012. Since 2012, Georgia has not introduced specific national cybersecurity laws. Therefore, information security policy in the country, mechanisms for state control of information security, and the responsibilities of controlling institutions are all still regulated under the abovementioned law of 2012.

## KEY ELEMENTS OF THE INFORMATION SECURITY LAW ADOPTED IN 2012

According to the Law on Information Security, minimum requirements for Information Security (Georgian adapted version of ISO/IEC 27001) were set out based on the **Order** of the Chairman of LEPL Data Exchange Agency on Minimal Security Requirements for Critical Information System Subjects. Additionally, the law on Information Security introduced a new term of **“critical information system subject”** (Article 2, Subparagraph “g”); hereby, the law defined the necessity of applying internal rules for information security to critical information system subjects and distinguished information security coordinating agencies among the civil and defense sectors.

According to the law, the scope of Critical Information System Subject covers a state body or a legal person whose uninterrupted operation of the information system is essential to the defense and/or economic security of the State, as well as to the maintenance of state authority and/or public life.

It is important to note that under the scope of the current legislation, the introduction of **minimum requirements** for Information Security and accountability to statutory agencies applies **only to legal entities and government agencies that represent the subjects of critical information systems.**<sup>1</sup>

The list of critical information system subjects was approved by an **ordinance** of the Government of Georgia of April 29, 2014, and covers 39 organizations, including administrative bodies that are institutionally completely independent from the Government of Georgia, namely: the Parliament of Georgia, the Administration of the President of Georgia, Tbilisi City Hall, the Election Administration of Georgia, the National Bank of Georgia, Georgian Railway, Sakaeronavigatsia Ltd. and others.

---

<sup>1</sup> Law of Georgia on Information Security, Article 3, Paragraph 1

The list of critical information system subjects in the field of defense was approved by a separate **act** of the Government of Georgia.

## ORGANIZATIONS RESPONSIBLE FOR INFORMATION SECURITY

In compliance with the current legal framework, information security system coordination and regulation management fall under the responsibilities of the Digital Governance Agency (formerly, the Data Exchange Agency). Meanwhile, the introduction and protection of the minimum standards of information security in the defense field are coordinated by the Cyber Security Bureau.<sup>2</sup>

### LEPL - DIGITAL GOVERNANCE AGENCY (FORMERLY, DATA EXCHANGE AGENCY)

According to current legislation and **National Strategy on Georgian Cybersecurity 2017–18**, the **Digital Governance Agency** is responsible for outlining minimum requirements and suggesting recommendations towards Information Security. Accordingly, the agency represents the authority in charge of both **regulating** and **overseeing implementation** of the policy.

### THE COMPUTER EMERGENCY RESPONSE TEAM (CERT.GOV.GE) OF DIGITAL GOVERNANCE AGENCY

The **Computer Emergency Response Team** functions under the subordination of the Digital Governance Agency and is responsible for the management of the incidents against information security in the cyberspace of Georgia, as well as other related activities aimed at coordinating information security that serve to eliminate priority cybersecurity threats.<sup>3</sup>

### The State Audit Office

Although the law does not specify the role of the **State Audit Office**, the institution has the mandate to conduct an **IT and information security audit** in any organization and to submit a report to the Parliament of Georgia on compliance with the requirements of the law.

### SPECIAL CYBERCRIME UNIT OF THE CENTRAL CRIMINAL POLICE DEPARTMENT OF THE MINISTRY OF INTERNAL AFFAIRS OF GEORGIA (MIA)

Since 2012, a Special **Cybercrime Unit** has been operating within the Central Criminal Police

---

<sup>2</sup> Law of Georgia on Information Security, Article 3, Paragraph 3;

Based on the reorganization on March 1, 2020 as a result of the merger of the Data Exchange Agency and SMART LOGIC, a new structure was established - the Digital Governance Agency. According to the legislative changes adopted on June 12, 2020, the new institute is the legal successor of both the Data Exchange Agency and SMART LOGIC and combines the functions and responsibilities of both organizations. Accordingly, the development and implementation of information and cybersecurity policy are coordinated by the Digital Governance Agency, within its competence and authority.

<sup>3</sup> Law of Georgia on Information Security, Article 8, Paragraph 1;

Department, Ministry of Internal Affairs of Georgia (MIA). The Unit is responsible for the detection, suppression, and prevention of illegal activities committed in cyberspace throughout the country.

The Unit also acts as an international focal point for the purposes of international police cooperation following the [Convention on Cybercrime](#).

### LEPL CYBER SECURITY BUREAU OF THE MINISTRY OF DEFENSE OF GEORGIA (MOD)

Since its establishment in 2014, provision of information and communication technology system security, as well as protection of information and communication technology infrastructure of critical information system subjects in the field of defense sector falls under the responsibilities of the **Cyber Security Bureau of the Ministry of Defense of Georgia**<sup>4</sup>. The Bureau carries out the study of existing infrastructure, as well as enhancement, operationalization, and development of computer security incident response mechanisms within the MOD of Georgia. Additionally, activities aimed at detecting/neutralizing cyber threats and cyber risks within the MOD also fall under the authority of the **Cyber Security Bureau**.

### STATE SECURITY SERVICE OF GEORGIA (SSSG)

The role of the State Security Service (SSSG) towards the protection of cybersecurity is not defined within the current legislation. At the same time, the activities of the Service in the field of cybersecurity and the measures taken to prevent or eliminate cyber-incidents and attacks are not highlighted at all in the **2018** and **2019** reports of SSSG. General information on the responsibilities and activities of SSSG in the field of information and cybersecurity can be obtained from the **2015 report** of the Service, quoting: *Protecting the security of the country's cyberspace does not fall within the authority of the State Security Service, however, given the scale of the threat and the severity of its expected consequences, the SSSG takes some measures to neutralize these threats, as well as to minimize the consequences.*

At the same time, according to the Criminal Procedure Code of Georgia, the **Operative-Technical Agency of the State Security Service** has the exclusive authority to conduct covert investigations into computer systems.<sup>5</sup>

### THE NATIONAL BANK OF GEORGIA

Based on the [Organic Law of Georgia on the National Bank of Georgia](#), the formats and standards concerning information security are established under an appropriate procedure by the National Bank within the scope of its authority<sup>6</sup>.

According to the [Regulation](#) of the National Bank of Georgia on Cybersecurity Management,

---

4 Law of Georgia on Information Security, Article 101, Paragraph 1;

5 Criminal Procedure Code of Georgia, Article 3, Paragraph 32, subparagraph "a";

6 Organic Law of Georgia on the National Bank of Georgia, Article 67, Subparagraph 2;

approved by the Governor of the National Bank of Georgia, the National Bank is the sectoral regulator of commercial banks in the field of cybersecurity. A cybersecurity framework based on the American NIST has been approved following the mentioned **Regulation** of the National Bank of Georgia on Cybersecurity Management. Under the framework, the National Bank has the authority to oversee the implementation of minimum information security standards set for commercial banks.

## **OFFICE OF THE STATE SECURITY AND CRISIS MANAGEMENT COUNCIL OF GEORGIA**

Following the 2013 constitutional reform, largely centralized approaches to national security issues were introduced, and cybersecurity shifted to direct subordination to the Georgian government. In particular, **the State Security and Crisis Management Council**, established in 2014, has been identified as the main coordinating body for cybersecurity policy.

In order to regulate cybersecurity, the **responsibilities of the Council covered developing a basic cybersecurity policy framework and making recommendations to the Government of Georgia on the development of a cybersecurity system**. At the same time, **the Council coordinated relevant agencies in the process of identifying cyber threats** and developed appropriate measures to neutralize and reduce said threats. The Crisis Management Council, principally during the crisis, was responsible for coordinating the work of all relevant agencies.

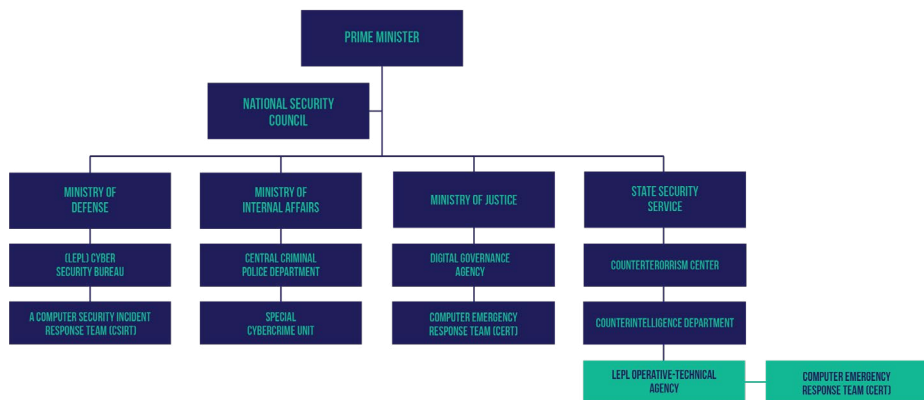
Per the amendments to the **Law of Georgia on the Structure, Authority and Rules of Operation of the Government of Georgia** of January 1, 2018, the State Security and Crisis Management Council was abolished and replaced by the Emergency Management Agency, subordinated to the Prime Minister. Further, based on the legislative changes of 2019, the National Security Council has been established as an advisory body under the Prime Minister of Georgia. The main purpose of the Council is to prepare policy decisions on issues threatening national security and state interests, to plan and coordinate national security policy at the strategic level, to prepare recommendations and decisions, and to keep the Prime Minister informed.<sup>7</sup>

According to the same law, information security is one of the most important directions of national security policy<sup>8</sup>. Accordingly, the functions of the Council also cover coordinating the implementation of information security policy. Specifically, the process of developing draft cybersecurity strategy as a major national conceptual document is conducted under the direct supervision and coordination of the Council. The Security Council represents the body that submits the draft strategy for approval to the Government of Georgia. Meanwhile, according to the strategy, the Digital Governance Agency is responsible for its implementation.

---

<sup>7</sup> Law of Georgia on the Structure, Authority and Rules of Operation of the Government of Georgia, Article 191;

<sup>8</sup> Law of Georgia on the Structure, Authority and Rules of Operation of the Government of Georgia, Article 3;



## CHALLENGES RELATED TO INFORMATION SECURITY AND LAW ENFORCEMENT

Implementing and managing an effective cybersecurity policy, ensuring implementation of and compliance with minimum standards, and addressing computer incident challenges is, above all, the subject of political will. Ensuring operational cybersecurity management system requires active support from relevant decision-makers, as well as infrastructural support and human resource readiness of the agencies.

One of the main challenges towards the implementation process of the Law on **Information Security** was the lack of prioritization of the information security field among the rest of the main directions of state policy. Challenges extended to the state of development of normative acts pertaining to the regulation of information safety and mechanisms for ensuring cybersecurity, as well as the normative basis for defining critical information infrastructure. Specifically, the Law of 2012 did not provide the proper legal framework for the activities of the support group working on cyber incidents; the responsibilities taken on as a result of the ratification of the 2001 Convention on Cybercrime could not be fulfilled in accordance with the law; simultaneously, reserve plans and procedures pertaining to cybersecurity were not fully defined. Thus, the Law on Information Security could not ensure proper implementation and monitoring of the newly adopted regulations.

One of the primary difficulties facing law enforcement and process coordination can be considered the fact that the **LEPL Data Exchange Agency (now, the Digital Governance Agency)** did not possess the authority or mandate to impose any kind of sanctions in cases where the law was not being met.

The effectiveness of cybersecurity policy is mainly measured by five main indicators: legislative framework, organizational arrangement, technical capabilities, capacity building and cooperation. The current reality shows that Georgia has not developed critical components of the cybersecurity system, which are prerequisites for effective response to cyber threats. According to international indexes, the integration of cybersecurity component into the education system

(primary schools, universities, doctoral programs), cyber incident reporting and cyber crisis management, information security management policy, legal and strategic framework, as well as cybersecurity analysis, national coordination and information exchange capabilities still remain the major challenges for Georgia.

The lack of a systemic legislative reforms of 2012 and the absence of a holistic approach to the development in the area of cybersecurity negatively affected Georgia's rating in the National Cyber Security Index (NCSI)<sup>9</sup>, according to which Georgia shifted from 19<sup>th</sup> spot to 47<sup>th</sup> spot on the list.

In any organization, whether public or private, management support is necessary when implementing information security and quality management systems. Especially for such a state, facing challenges such as a fragile cybersecurity environment and less protected cybersecurity mechanisms, it is essential to prioritize the field and provide state or international support in the process of systemic reforms.

In the context of increased cyber-attacks, as demonstrated by **the attack in October 2019**, during which the websites of the President, courts, Municipal Councils, and media outlets were attacked and taken down, it is clear that cybersecurity should become one of the top priorities for the state. Effective steps need to be taken to prevent high-tech unlawful interventions and minimize existing threats.

IDFI requested from the State Audit Office of Georgia acts of inspection of the critical information system subjects in connection with the implementation of the Law of Georgia on Information Security through 2013-2020, as well as recommendations issued by the Office. The audit report provided upon request proves that adhering to cybersecurity policies and enforcing the requirements of the law has not been a priority for the **39 government agencies identified as critical information system subjects. The report revealed that most of these institutions had not adopted internal rules for information security. Additionally, information security policy had not been approved in compliance with the minimum requirements for information security. The information security manager (if any) had been only a position of formality and could not meet the requirements of the law.**

Based on the report, it is clear that control mechanisms exist only as a formality and do not enable the fulfillment of responsibilities. Several instances can be seen as an example:

1. The audit report on the effectiveness of the Public Debt Management information systems shows that the draft information security policy, elaborated by the institution, has not been approved by the management, and hereby, does not meet minimum requirements of information security.
2. The audit report of the Education Management Information System (EMIS) revealed that the field of information security management system (UMS) faces obvious challenges with regards to the distribution of governance and monitoring powers and the provision of appropriate human resources for the UMS implementation process.
3. The audit report of the Administering Pensions Information System shows that the Social

---

<sup>9</sup> National Cyber Security Index. Available at <https://ncsi.ega.ee/ncsi-index/>

Service Agency has not assessed the risks related to the continuity of the system and appropriate control mechanisms have not been introduced. This problem is reflected in the difficulty of transmitting a special category of personal data through a secure line. For example, the use of an unprotected communication channel when receiving special categories of personal data from the Special Penitentiary Service. This is contrary to the requirements of the legal framework and does not meet minimum standards.

**The recommendations of the State Audit Office are addressed to the critical information system subjects** and require the development and implementation of the information security management system following the existing legal framework. Recommendations suggested to the government include the following directions:

- **Giving the Data Exchange Agency additional authority to enforce legal requirements related to information security, including following international practices, the power to impose sanctions to critical information system subjects.**
- **Introducing a mechanism for the application of sanctions against critical information system subjects only following international practices and based on international experience.**
- **Implement effective mechanisms for identifying accurate and relevant critical information system subjects and imposing an obligation for periodic review of the list of critical information system subjects.**

Analysis of the State Audit report confirms that the state already possesses the knowledge and experience necessary for conducting information security audits and monitoring the management of the information security system. However, the listed recommendations as well as the role of the State Audit Office have not been considered in the process of elaborating draft **amendments to the Law of Georgia on Information Security**, initiated by MP Irakli Sesiashvili in October 2019, that will be discussed later in the report.

Achieving the main purpose of developing efficient information security and cybersecurity systems requires legal reform to be based on thorough analysis of the problems identified in practice; study of the international legal framework and harmonization with best practices should be ensured. The process of undertaking legislative changes and establishing new realities of field management as a whole needs to derive from problem analysis and should consider the knowledge already accumulated towards field management in the state. **Given the specificity of the information security management and evaluation process, it would be desirable to use the human and theoretical resources already available in the State Audit Office and to take the above recommendations into account.**



**RISKS AND CHALLENGES RELATED TO THE AMENDMENTS  
TO THE LAW OF GEORGIA ON INFORMATION SECURITY**



## SUMMARY OF THE PROPOSED CHANGES

The work towards further developing the legal framework on Information Security resumed on October 2, 2019, as Georgian MP Irakli Sesiashvili introduced a new legislative initiative to amend the Law on Information Security. However, the initiative encountered widespread criticism from experts, non-governmental organizations, and the private sector.

The proposed bill has been criticized for several important **reasons**: 1. The fundamental changes introduced by the bill create a risk of unbalanced control of the information security system; 2. Legislative changes do not take into account international practices and experience; 3. Initiation of the changes was not preceded by extensive consultations with stakeholders, resulting in the legal amendments shifting the country's cybersecurity architecture with no regard to common consensus.

The bill has come a long way since its registration. Due to disagreements with stakeholders on fundamental issues, the legislative changes were also returned to the mode of second reading from third reading.<sup>10</sup> The current version differs significantly from its originally conceived version, although it still includes problematic circumstances, which raises quite a lot of questions in terms of the effective and balanced implementation of the law.

Amendments to the Law on Information Security cover three key dimensions: 1. The amendments concern the categorization of Critical information system subjects, and the scope of the law is expanded to include the subjects of the private sector under the regulation; 2. The state axis of coordination and management of the information security system is planned to be shifted; 3. The coordinating and supervising agency for ensuring information and cybersecurity by the critical information system subjects is substituted.

## PROBLEMS RELATED TO CATEGORIZATION OF THE SUBJECTS OF CRITICAL INFORMATION INFRASTRUCTURE

According to the explanatory note of the draft law, the main aim of the amendments is to introduce a new system of categorization for the objects of critical information infrastructure and introduce new oversight and administrative liability mechanisms applicable to them. However, the draft does not clearly state the basis and criteria for categorizing critical information system subjects.

The draft amendments introduce the following three-tier categorization for the objects of critical information infrastructure (three tiers):

- a) Tier 1 – state agencies, institutions, LEPLs (other than religious organizations) and state enterprises;
- b) Tier 2 – electronic communication companies;

---

<sup>10</sup> "Draft law on Amendments to the Law on Information Security Returned to the Second Hearing". Institute for Development of Freedom of Information (IDFI). available at: <https://idfi.ge/ge/idfis-statement-about-the-draft-law-on-information-security>

c) Tier 3 – banks, financial institutions, and other entities of private law.

Based on the proposed version of the Draft Law on Amendments to the Law of Georgia on Information Security, a new entity appears in the architecture of information security policy regulation, the Operative-Technical Agency (OTA), which represents a LEPL, a subordinate body of the State Security Service (SSSG). According to the amendments, the OTA will coordinate the critical infrastructure subjects of the first and the second category, while the third category of critical information system entities will partially remain under the umbrella of the Digital Governance Agency (formerly the Data Exchange Agency) as the National Bank oversees and regulates the information security of commercial banks.

Although the draft law suggests differentiated approaches towards the responsibility and Information Security System Management Oversight of the entities falling under the first, second and third categories of critical information subjects, the following key aspects remain problematic and ambiguous:

- Under the proposed amendments, in the case of the subjects of the first category, the Operational-Technical Agency is granted full access to information assets, information systems and infrastructure of the institutions, as OTA is given the leverage to control the sensor located in these institutions as well as the network of the institution. This is justified by computer incident identification purposes.
- The guiding principle according to which private sector organizations were classified as entities falling under Tier 3 and Tier 2 critical information infrastructure subjects is wholly unclear. The subjects of the second category of critical information infrastructure, i.e. the telecommunication companies, are obliged to submit internal rules for information security for consideration to the Operational Technical Agency, while the sectoral regulator in the form of the National Bank maintains supervision over the entities under the scope of the third category.
- The inclusion of electronic communication companies under the categorization of the subjects of the critical information system is in direct conflict with the separate requirements of the Network and Information Systems (NIS) Directive (discussed in detail below, in the section of the Legislative Amendments Directive and the Association Agreement).
- Adding the second and third category entities to the hierarchy of critical information system entities may result in increased bureaucracy for the private sector. In particular, in some cases, banks and **financial institutions retain some accountability to the Digital Governance Agency. Consequently, there is a possibility of duplication of responsibilities in various aspects between the two regulators, the National Bank and the Digital Governance Agency.**

## THE EXCESSIVE MANDATE OF LEPL OPERATIVE-TECHNICAL AGENCY OF THE STATE SECURITY SERVICE ACCORDING TO THE DRAFT LAW

In case the current version of the draft law is passed, we will get a new information security

policy architecture under the control of a centralized law enforcement agency. Full access to information systems of state institutions will be transferred to the State Security Service.

In particular, the existing cybersecurity architecture will be changed drastically and the State Security Service LEPL Operational-Technical Agency (OTA) will in fact become the main coordinator and supervisor of information and cybersecurity in the case of the entities of the first and second categories of critical information infrastructure, as the OTA will be equipped with the broad powers to:

- Configure and coordinate the network sensor installed at the institutions of the first and second category (with consent) of the critical information system subjects in order to monitor network flow;
- Access information assets, information systems and / or information infrastructure upon request, if such access is necessary to respond to current or previous computer incidents in the case of the entities of the first and the second categories;
- To carry out inspections of information technology infrastructure in a mandatory, planned or unplanned manner;
- To determine administrative legal responsibility / sanctions in case of non-fulfillment of the conclusion developed as a result of the inspection;
- To establish minimum requirements for information security for the first and second categories of critical information systems under the sublegal act;
- To consider internal rules for information security in the case of the subjects of critical information systems under the first and the second categories;
- Request information from a critical information system entity regarding the development, implementation, monitoring and improvement of information security policies.

As a result, in the case of the first and second category entities, the SSS LEPL Operational-Technical Agency (OTA) will be assigned the functions of a regulator, accreditation holder and executive body.

It should be noted that the bill as presented at the first reading turned out to be radically unacceptable for entities of the third category (financial institutions), as the information assets of private financial institutions were, in fact, under the direct risk of control and supervision by the law enforcement agency.

In the currently proposed version, entities of the third category, namely commercial banks and private financial institutions, remain under supervision of the National Bank as a sectoral regulator and have only minimal accountability to the Digital Governance Agency. This applies to: a) the authorization of the list of organizations able to conduct the penetration / audit test submitted by the National Bank, b) submission of the penetration test report to the Digital Governance Agency and c) introduction of internal policy documents.

However, changes in the updated version did not affect the telecommunications sector (second category entities). Consequently, coordination and supervision of the management of the

information security system of the electronic communications companies remain under the umbrella of the OTA. According to the draft amendments, in order to avoid the danger of a recurrence of a computer incident, the Computer Incident Assistance Team of the Operational-Technical Agency (CERT.OTA.GOV.GE) is empowered to imperatively request the electronic communications company in question to take necessary measures in order to identify and neutralize similar computer incidents in its infrastructure. Failure to do so entails administrative responsibility, which might render objects falling under tier 2 more vulnerable to OTA, as they would be more likely to grant OTA access to their infrastructure, including network sensors, to avoid fines. The potential increase of the powers of the security sector without strict regulation creates increased risks of state intervention in an area protected by fundamental rights; particularly, risks of obtaining, processing, and studying information about an unidentified group of persons.

The State Security Service is, in fact, a law enforcement agency that, for security purposes, has a direct interest in having maximum access to various information infrastructures. It will easily be able to satisfy this interest if it is equipped with legal mechanisms for issuing by-laws.

**Given existing hybrid threats and increased risks of cyber-attacks, the purpose of the legislative amendments and legal reform should be strengthening investigative and incident elimination mechanisms, rather than creating ineffective information security architecture and justifying the risks of obtaining total control over information systems and assets of public/private institutions.** The proposed changes create several institutional and organizational inconsistencies, namely:

- a) Increased risk of unreasonable access to information assets of the objects of the first and second category, and enlarged capacity for processing protected data, giving the OTA direct access to information assets of legislative, executive and judicial authorities, various public agencies, including the CEC, as well as the information system of the telecommunications sector, and indirect access to personal and commercial information stored in the systems of above-mentioned organizations.
- b) Under the draft law, the law enforcement agency is given legal leverage to access personal data without the permission of the court, as the ambiguity of the norms poses a real danger of illegal and disproportionate processing of personal data.

## COMPLIANCE OF THE PROPOSED LEGISLATIVE AMENDMENTS WITH THE REQUIREMENTS OF THE ASSOCIATION AGREEMENT WITH THE EUROPEAN UNION

It should be noted that the proposed amendments to the law on Information Security contradict specific requirements of the **European Directive on the security of network and information systems (NIS Directive)**. In particular, under the Directive, **Member States are required to develop and implement a national cybersecurity strategy**. The strategy should include a common security standard, a common policy implementation strategy, and mandatory regulations.

The directive requires the strategy to define the following: a governance framework, response, and rapid recovery measures, coordination and cooperation plan between operators of essential services, digital service providers, competent authorities and law enforcement authorities, security awareness-raising programs, a risk assessment plan, and a list of identified operators of essential services responsible for implementing the strategy.

**The approach of the NIS Directive to the categorization of critical information system entities is particularly important. As mentioned, the Directive distinguishes two categories of entities and sets out different approaches and responsibilities for essential service operators and digital service providers.** The Directive also calls on States to adopt objective and quantitative national criteria for the identification of critical information system subjects to which security obligations and requirements will apply.

The Directive also emphasizes that digital service providers, for NIS, **do not include digital service providers and entities that fall under the category of “micro and small enterprises (with micro and small business status)”**. Such entities are not subject to the regulations and rules laid down in the Directive in the area of information security standards and computer incident reporting. The grounds for granting an organization micro- and small enterprise status are defined in the Commission Recommendation 2003/361/EC.

**It is also important that telecommunications companies are not subject to security standards set under the Directive and do not fall under the obligation to report computer incidents.** It is also important to note that under the Directive, telecommunications companies are already subject to the Directive № 2002/21 / EC on the General Regulatory Framework for Electronic Communication Networks and Services and are not covered by the NIS Directive.

It is noteworthy that the **government has not yet approved a new National Cyber Security Strategy of Georgia**, the development of which was supported by the international community. Number of activities envisaged in the Action Plan of the current working version of the Strategy run counter to the amendments proposed by the draft law. Specifically:

- One of the activities of the Strategy Action Plan refers to updating the Law of Georgia on Information Security and its by-laws for the purposes of harmonizing legal framework with the NIS Directive, whereas certain elements of the categorization of entities proposed by the draft amendments (for example, extension of cybersecurity requirements to telecommunications companies) are in conflict with the requirements of the Directive;
- According to the working version of the strategy, the agency responsible for refining and harmonizing the regulatory framework with the directive is the Data Exchange Agency (now the Digital Governance Agency), while the LEPL Cyber Security Bureau and the State Security Service are considered only as partner agencies. According to the bill, SSS will become one of the main actors in the country's cybersecurity architecture.
- The deadline for the implementation of the activities of the Strategy Action Plan is set for the third quarter of 2021, therefore, the adoption of the law in September 2020 will completely change the principal and important part of the strategy.

Hereby, the draft amendments and accompanying regulations directly contradict certain

requirements of the NIS Directive, as well as the obligations under the Association Agreement. The suggested framework is in conflict with the rules set out in the General Data Protection Regulation (GDPR) pertaining to the processing of personal data. The drafting process did not ensure compliance with the above-mentioned regulations and to date no relevant measures have been taken to this end.

## LACK OF ENGAGEMENT

At the same time, the drafting process was not inclusive. Proper engagement of various stakeholders, including civil society, field specialists, and the private sector was not ensured. It is also unknown whether an in-depth study of international practices and standards took place before the amendments had been elaborated. Since the first reading, some recommendations of civil society representatives were considered to some extent. IDFI also published a **statement** on the proposed version for the second reading, reviewing editorial and substantive changes reflected in the new version of the bill. Despite the initiators considering the recommendation to narrow the scope of several terms, substantial and principal issues remained unaddressed during the second reading of the draft amendments.



## CYBERSECURITY ARCHITECTURE: INTERNATIONAL EXPERIENCE

## INTRODUCTION

The purpose of this part of the study is to explore international experience regarding information security architecture, critical infrastructure, legal framework, and information security regulations.

The study was conducted using open source materials and included countries such as the United States of America (USA), the United Kingdom (UK), Estonia, Germany, and France. The study also covers the EU Directive on Security of Network and Information Systems (the NIS Directive) concerning the identification and management of critical infrastructure. The countries were selected based on the following criteria: critical infrastructure identification model, incident management and response capabilities, cyberspace organizational arrangement and coordination mechanisms, and legal framework.

The study has shown that in order to ensure cybersecurity, cyberspace architecture must include several important components, such as Organizational arrangement; Critical infrastructure; A transparent and well-organized supervision, information exchange and accountability system; Sophisticated mechanisms for classification and response to cyber incidents.

Organizational arrangement is the most important part of the architecture, which should consist of a coordinating agency at the national level, a National Cyber Incident Response Team, and an agency responsible for the security of military networks and systems within the Ministry of Defense.

According to the NIS Directive, all EU member states are required to designate one or more authority (Competent Authority) responsible for the proper functioning of critical infrastructure. It should also be noted that the **Directive does not specify whether it should be a police agency, a security organization, or a civilian office**. All countries have the right to assign this function to an agency they deem necessary. In the case of the US, the UK, France, and Germany, this function is assumed by security-type organizations, while in the case of Estonia, the security of cyberspace is the responsibility of a civilian agency. Military cyber defense of all countries surveyed is a responsibility of their respective defense institution.

According to the study, managing critical infrastructure involves identification of critical sectors, services, service providers and establishment of appropriate information security standards for them. In all given countries, identification of critical infrastructure is carried out on a sectoral basis, under pre-designed criteria, such as probability of critical service failure and extent of potential damage. NIS regulation does not apply to small businesses and organizations with fewer than fifty employees.

In all given countries a transparent and well-organized system of supervision, exchange of information, and accountability have been introduced. Supervision is carried out by strictly prescribed procedures, and competent authorities have no right to interfere in the activities of the entities that are not related to the provision of information security. They do not have access to the entity's networks unless the incident poses a threat to public health and national security. According to the study, these countries have developed clear models for classifying cyber incidents as serious or minor. Serious incidents are reported to critical authorities immediately



or in a predefined timeframe; otherwise, the responsibility of the first-line responder falls to their IT staff.

Entities should comply with the requirements of the competent authority. Otherwise, they will face an administrative penalty.

## **BUDGET AND PRIORITY**

A study of international cybersecurity experience revealed that all represented countries have devoted a substantial portion of their budgets to cybersecurity. In Georgia, cybersecurity issues are only prioritized in conceptual and strategic documents, but not in practice. Consequently, limited resources (financial and intellectual) are allocated to its development. We should consider the fact that cybersecurity is an area in which a country cannot operate successfully without proper funding.

## **NATIONAL STRATEGY**

The study showed that all developed countries have a national cybersecurity strategy - the main conceptual document for ensuring cybersecurity, which outlines existing challenges and an action plan. Currently, Georgia has not approved a National Cyber Security Strategy. Moreover, the draft law on Information Security is inconsistent with the current draft version of the strategy. The manner in which the draft law regulates responsibilities for ensuring cybersecurity, changes the list of critical infrastructure, and introduces administrative-legal sanctions differs from the current draft version of the strategy.

## **INSTITUTIONAL FRAMEWORK**

The study shows that ensuring cybersecurity is a shared responsibility, and both the public and private sectors make a concerted effort to prevent and manage cyber incidents.

In all surveyed countries, except Estonia, a specific security organization is responsible for cybersecurity at the national level. In the case of the US, this kind of organization – DHS, is subordinate to the Secretary of State; in the case of the UK (GCHQ) and France (ANSSI) - the Prime Minister; in the case of Germany (BSI) - the Minister of the Interior; and in Estonia (RIA) - the Minister of Economy and Communications.

## DEFINING CRITICAL INFRASTRUCTURE

In the countries surveyed, critical sectors are identified according to their impact on the functioning of the country. Cybersecurity of critical entities identified in the critical sectors is the responsibility of the sector regulator, which is in turn accountable to the national agency.

The study showed that the **existing classification of critical information system subjects does not fit either the European or the American model**. The new model does not meet the requirements of the EU Directive (NIS Directive), according to which critical entities are classified according to the sectoral principle based on the rate of impact on the effective functioning of the state. For comparison, according to the new legislative proposal submitted to the Parliament of Georgia, subjects of the critical information system are divided into three parts, while the critical infrastructure of developed countries is usually divided into several sectors and sub-sectors.

**Another legislative shortcoming is the lack of criteria for identifying critical information system entities.** These entities, sectors, or areas are identified according to the probability of possible damage and the severity of the consequences, according to strictly defined criteria, such as scale of the damage to economic and social activities and security of the country. The scale of damage is assessed by criteria such as the market share of the affected organization, geographical area of distribution, etc. **Small operators, which do not meet the above criteria, are not considered critical entities.**

**The name of the law and definition of the critical infrastructure itself can also be considered a legislative shortcoming.** According to European, American, and international standards, important areas and sectors for the proper functioning of the country are defined under one internationally recognized name - **critical infrastructure, which includes the so-called virtual as well as physical infrastructure**. According to the legislation of Georgia, critical infrastructure includes only virtual infrastructure, which is also indicated by the name – “subjects of the critical information system”. **Information security is a broad term and includes the security of both physical and virtual assets.** Information security cannot be ensured without secure infrastructure. Consequently, the term introduced in the law of Georgia - “subject of a critical information system” - does not fit with internationally recognized practices.

## ACCESS AND MONITORING

Although the main cyber actors in the surveyed countries are security-type organizations, the study does not indicate that they tend to have any means and tools to directly manage critical assets of critical infrastructure entities. The study showed that these agencies impose security requirements on critical infrastructure sectors, the fulfillment of which is mandatory for all of them, be they public or private.

The national agency does not have direct access to the entities unless the national agency itself is the regulator of the critical sector.

Moreover, in the mentioned countries, the government sector is overseen by the national

agency itself. Therefore, it has access to government infrastructure. In other cases, as already mentioned, the national agency has access to the sector infrastructure, but directly interferes only in cases where the incident is so significant as to threaten national security.

This organizational structure is not violated during an audit. In critical entities, an audit is conducted by the sector regulator following procedures prescribed by the national agency. In the government sector, periodical audits are conducted by the national agency. The frequency and procedures of the audit are described in a separate order and are not unscheduled.

In all of the surveyed countries, the size of the organization is taken into consideration when identifying critical entities. For example, in the case of the EU, digital service providers with an annual turnover of less than EUR 10 million and/or with less than 50 employees are not covered by the NIS Directive.

The study of international experience shows that, in some cases, the proposed amendments to the Law on Information Security of Georgia completely lack aspects of the worldwide best practices in this sphere.

## CLASSIFICATION OF INCIDENTS

**The lack of a classification of cyber incidents at the national level can also be considered a legislative shortcoming.** According to international practice, all incidents identified in critical infrastructure information systems are sorted (incidents are sorted by critical and possible damage levels), and a response is carried out according to a pre-designed incident response scale and plan. There is no such classification of incidents at the national level in Georgia, which has a negative impact on the quality of security.

Under Article 9, Paragraph 2, Subparagraph B of the Draft Law on Information Security, in case of cyber incidents, the critical information system subject should immediately inform the relevant agency. International experience has shown that critical infrastructure entities, in coordination with the Computer Security Incident Response Team (CSIRT) of the relevant coordinating agency, **exchange information only on cyber incidents that affect the normal functioning of these entities.**

In all surveyed countries, incidents are classified according to the probability of occurrence and possible damage, and therefore the supervisory authority is provided with information only on “significant” incidents and not all cyber incidents. Which incident is “significant” and which is “less significant” is determined by a separate legal act. The same rules should apply to the Georgian case as well. **It should be noted that neither the OTA nor the Digital Governance Agency or the Cyber Security Bureau has sufficient human and technical resources to analyze and respond to all cyber incidents that occur in critical information system subjects. Therefore, this article needs to be amended further.**

## MILITARY CONFLICT

According to paragraph 5 of article 9 of the draft law, during the state of war, cybersecurity and cyber operations are carried out under the Law of Georgia on the State of War. **The final version of the “Law of Georgia on Martial Law” does not contain any article that describes how to ensure cybersecurity in the country during the state of war or how to coordinate responsible agencies and repel massive cyber-attacks.** Therefore, it is vital to take certain measures in this direction, especially if we keep in mind the fact that **Georgia has repeatedly become a victim of massive cyber-attacks, to which state agencies have failed to show an appropriate level of coordination and response.**

## PROTECTION OF PERSONAL DATA

In many cases, personal data is compromised as a result of incidents. Accordingly, the Operative-Technical Agency and the Digital Governance Agency should cooperate with the State Inspector’s Service in order to ensure security of personal data. **The Law of Georgia on Information Security does not include a mention of the inviolability of personal life and protection of personal data.**

The NIS Directive emphasizes that incidents reported to CSIRT by critical entities may include personal information, and processing of such information should be in line with Directive 95/46/EC and Regulation 45/2001 of the European Parliament and the Council of Europe. The information exchanged should be limited to information that is relevant and proportionate to the purpose of the investigation of a cyber incident or the reaction to it. Such an exchange of information shall preserve the confidentiality of the information, the security of the operators of basic services and digital service providers, and commercial interests.

## AUDITING AND TESTING

International experience has shown that the subjects of critical infrastructure themselves take appropriate technical and organizational measures to manage security risks posed by networks and information systems, including:

- Network security
- Incident management
- Business continuity management
- Compliance with international standards
- Monitoring, auditing and testing

According to Article 6 of the draft Law of Georgia on Information Security, the audit and testing of

the appropriate entity is carried out by the Operative-Technical Agency, the Digital Governance Agency, or an organization authorized by the Digital Governance Agency. **This contradicts both the NIS directive and international practices.** For example, the UK Communications-Electronics Security Group is a national technical body that provides **advice, recommendations and, if necessary, assistance** to critical infrastructure entities, all with the goal to protect the security of their critical assets and networks.

## ACCOUNTABILITY AND TRANSPARENCY

Accountability and transparency of the government are important principles of a democratic state. Georgia has the ambition to become a full member of the European and Euro-Atlantic family. Therefore, the functioning of the country should be based on these principles. Cyber security is an important component of national security and, consequently, there is a high public interest in ongoing processes in this area.

It is vital that the Law of Georgia on Information Security include accountability procedures of the Operative-Technical Agency, the Digital Governance Agency and the Cyber Security Bureau in order to ensure transparency of cyber security efforts in the country, in accordance with international best practices and experience and with maximum involvement of the civil sector.



## POLICY RECOMMENDATIONS

The legislative changes initiated by the Member of the Parliament of Georgia, Irakli Sesiashvili, completely change the cyber architecture of the country and regulate critical infrastructure management issues in a new manner. Based on research of international practice, we will highlight issues that need to be considered and addressed to ensure a more secure cyberspace.

## COMPLIANCE BETWEEN THE NATIONAL CYBER SECURITY STRATEGY AND LEGISLATION

With the active involvement of international partners and all stakeholders, a draft of the National Cyber Security Strategy has been developed that responds to the challenges facing the country in this field. It is of utmost importance that this strategy be approved. Therefore, any new legislative initiative, including the Draft Law on Information Security, should be in line with the National Cyber Security Strategy.

## CYBER SECURITY MANAGEMENT MODEL

The National Security Council is currently responsible for the development and implementation of the country's cyber security policy, management of cyber crises, and coordination of appropriate agencies. However, it is necessary to set up a specialized unit staffed with cyber security specialists to coordinate matters of cyber security.

At the same time, if the Digital Governance Agency is appropriately equipped with hardware, software and personnel, the Agency will be able to ensure the security of the country's critical infrastructure in coordination with the State Security Service, Cyber Security Bureau, and the National Security Council.

Therefore, it is important to maintain the existing model of ensuring cybersecurity and to assign the function of overseeing the country's critical infrastructure to the Digital Governance Agency. By assigning this function to the OTA instead, the Agency is being given additional leverage of public control, which may increase the risk of restriction and/or violation of personal rights and freedoms on the Internet.

## CLASSIFICATION AND REPORTING OF CYBER INCIDENTS

It is necessary to classify cyber incidents based on their probability and possible damage in addition to developing cyber incident reporting procedures.

It is important to establish a platform for the secure exchange of information between supervisory agencies and critical infrastructure entities, through which sensitive information will pass, in order to prevent and respond to cyber-attacks in a coordinated manner.

## IDENTIFICATION OF CRITICAL INFRASTRUCTURE

It is of vital importance to define the criteria for identifying critical infrastructure on a sectoral basis. This will allow us to protect specific areas more effectively. When identifying critical

infrastructure, following criteria must be taken into consideration:

- The importance and role of the organization (governmental or private) in implementing and maintaining social and/or economic activities;
- Degree of dependence on network and information systems;
- In the event of an information security incident, the level of damage caused by the organization's disruption of service delivery.

When identifying critical infrastructure, it is important to consider the requirements of the NIS Directive, such as the probability of critical service failure and the extent of potential damage. Critical infrastructure regulations should not apply to small businesses and organizations, whose failure or alleged damage does not endanger national interests and the proper functioning of the country.

### THE ROLE OF THE NATIONAL SECURITY COUNCIL AND CRISIS MANAGEMENT

The National Security Council Charter states that one of the main areas of the Council's work is analysis of national security policies, including information security policy, identification and assessment of threats, and planning and coordination of policies. The Council also ensures proper coordination between state agencies in times of crisis.

The Georgian draft law on Information Security must include an article emphasizing the role and functions of the Council as the coordinator of the country's cyber actors. In this way, the Council will be able to carry out its functions, which will be an important supporting factor for the implementation of coordinated and synchronized actions during crises.

### PROTECTION OF PERSONAL DATA

As a result of information security incidents, personal data is compromised. Accordingly, cybersecurity policy enforcement agencies should cooperate with the Office of the State Inspector's Service to prevent breaches of personal data. The Draft Law on Information Security must include a provision related to the protection of personal data.

### PRIORITIZING CYBERSECURITY FIELD AND ALLOCATING APPROPRIATE FINANCIAL RESOURCES

It is important to make cybersecurity a priority for the state and to spend more financial and intellectual resources on its development.

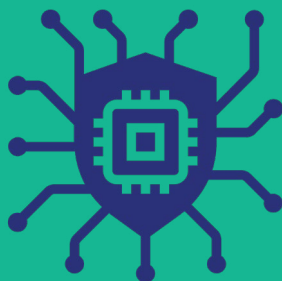
### PROVIDING PUBLIC CONTROL MECHANISMS

Given the high public interest, it is no less important to have public control mechanisms over the agencies involved in ensuring cybersecurity. This may be implemented through the following activities:



- Government agencies should implement their activities based on open government principles.
- Ensure the involvement of all stakeholders, including the non-governmental sector, in the development of cybersecurity policies and legislative changes.
- Implement consistent reporting on activities that have been carried out.
- Use the resources of the private and non-governmental sectors in trainings and cyber exercises.
- Organize regular meetings and exchange information on new initiatives.
- Involve non-governmental and private sectors in various educational and awareness-raising activities.

Implementing the recommendations outlined above and continued development of its cyber capabilities will make Georgia adequately protected against cyber threats.



**ANNEX 1: CYBERSECURITY REGULATORY FRAMEWORKS:  
INTERNATIONAL PRACTICE**



THE UNITED STATES

## CYBERSECURITY COORDINATION AT THE NATIONAL LEVEL IN THE US

Cybersecurity responsibilities in the US are spread across a wide range of agencies. The key policy coordinator is the National Security Council's Information and Communications Infrastructure Interagency Policy Committee (ICI-IPC). ICI-IPC is chaired by the Homeland Security Council and the Cyber Security Coordinator of the National Security Council. The Cyber Security Coordinator oversees development of national cybersecurity strategies and policies at the inter-agency level, as well as implementation of these policies by other entities.

The Department of Homeland Security (DHS), established by the Internal Security Act of 2002, is the primary institution responsible for cybersecurity in the United States. Its other duties include: strengthening the security and sustainability of critical infrastructure; assisting federal civilian agencies in cybersecurity procurement; strengthening law enforcement and responding to incidents. Cybersecurity and Infrastructure Security Agency (CISA) under DHS responds to cyber incidents, safeguards the gov. domain and protects critical infrastructure. DHS manages the Computer Emergency Response Team of the US (US-CERT).

The National Security Agency (NSA) has an important role in ensuring the country's cybersecurity. The Agency conducts cyber threat assessment and analysis, provides recommendations on the introduction of modern cyber intelligence and other technical capabilities, develops guidelines for network security and other solutions.

The Department of State (DoS) is the main body providing communication and coordination of the President's cybersecurity policy at the international level. Meanwhile, the Department of Justice (DOJ) is responsible for developing the legal framework related to cybersecurity, investigating and prosecuting cybercrime, gathering intelligence, and providing legal and political assistance to other agencies. The DOJ investigates and suppresses cybercrime within its jurisdiction and conducts domestic national security operations related to cyber threats, including the prevention of threats from foreign intelligence and terrorism, in addition to other national security issues.

The Department of Defence (DOD) is tasked to protect the "MIL" domain and the DOD's global information infrastructure from cyber-attacks. US Cyber Command (USCYBERCOM), whose primary task is to centrally manage and control cyberspace operations, reports directly to the DOD.

## CRITICAL INFRASTRUCTURE PROTECTION IN THE US

There are 16 critical infrastructure sectors in the US, whose assets, systems, and networks, whether physical or virtual, are vital for the proper functioning of the US national and economic security, public welfare, and defense. **All critical sectors have a corresponding authority overseeing them, although DHS is responsible for ensuring cybersecurity in most of them, including the government sector.**

The Critical Infrastructure Information Act regulates the procedures for the exchange of information between the DHS and the critical infrastructure sectors. Under the law, DHS has set up an Information Analysis and Infrastructure Protection Directorate responsible for receiving and processing information from critical infrastructure entities. According to the law, any

information received from entities is protected from unauthorized disclosure and is used solely to perform official duties, such as the prevention, identification, and response to cyber threats. Any critical information related to critical infrastructure is obtained, processed, and used with the consent of the Central Intelligence Agency (CIA) and the Attorney General.

The Directorate is empowered to create and operate secure information and communication infrastructure (secure channels for information exchange), and to use various advanced analytical and technical tools to access, receive, and analyze data for further response. The Directorate exercises this authority in full compliance with the norms of personal data security and Federal legislation.

The Directorate has access to all types of information stored in critical infrastructure entities that it deems necessary, including reports, evaluation documents, any kind of analytical material, including intelligence, and all information related to critical infrastructure or any federal agency. This information is provided to the Secretariat upon request or on a voluntary basis.

Acquisition of sensitive information, for example, in the case of the banking sector, must comply with the regulations on the exchange of sensitive banking information, and DHS is required to comply with these regulations. The processing and use of the received information are regulated by an additional legal act.

Federal law obliges all critical infrastructure entities to implement appropriate security mechanisms and to comply with DHS regulations. Failure to comply with these obligations is punishable by federal law, **based on the importance of the rules that had been violated and the consequences of such violations.**

#### Critical Infrastructure sectors and responsible agencies of the US:

SECTOR	RESPONSIBLE AGENCY
Chemical	DHS
Communications	DHS
Dams	DHS
Emergency services	DHS
Financial services	Department of Treasury
Government facilities	DHS
Information Technology	DHS
Transportation	DHS
Commercial facilities	DHS
Critical manufacturing	DHS
Defence industrial base	Department of Defence
Energy	Department of Energy
Food and agriculture	Department of Agriculture and the Department of Health and Human Services
Healthcare and public health	Department of Health and Human Services
Nuclear reactors, materials and waste	DHS
Water and wastewater systems	Environmental Protection Agency

## INCIDENT CLASSIFICATION METHOD

Concerning incident classification, according to the “Cybercrime Coordination Directive” issued by the President of the United States, cyber incidents are classified as follows:

INCIDENT	DESCRIPTION
<b>CYBER INCIDENT</b>	<i>An event that takes place in a computer network, or is carried out through a computer network, and endangers (or inevitably will endanger) the privacy, integrity, or accessibility of physical or virtual infrastructure controlled by computers, networks, information or communications systems.</i>
<b>SIGNIFICANT CYBER INCIDENT</b>	<i>An incident (or combination of incidents) that may cause particular harm to a country’s national interests, international relations, economy, society, the health, safety, and liberty of the American people.</i>

The US Federal Cyber Security Center has developed a five-tier classification of cyber incidents that is shared across all critical entities in the country.

LEVEL OF A CYBER-INCIDENT	DESCRIPTION
<b>LEVEL - 5 Critical</b>	Poses an imminent threat to the proper functioning of critical infrastructure services, the stability of government, or the lives of U.S. citizens.
<b>LEVEL - 4 Extremely High</b>	Most likely will threaten public health or safety, national security, economic security, international relations, or human rights.
<b>LEVEL - 3 High</b>	It is likely to pose a significant threat to public health or safety, national security, economic security, international relations, or human rights.
<b>LEVEL - 2 Medium</b>	It may have an impact on public health or safety, national security, economic security, international relations, human freedoms, public confidence.
<b>LEVEL - 1 Low</b>	It is less likely to endanger public health or safety, national security, economic security, international relations, human freedoms, public self-confidence.
<b>LEVEL - 0 Basic</b>	Random and inconsistent cases.

According to this classification, third level (and above) incidents belong to the category of “significant incidents”. These warrant the formation of a **unified coordination group**, which is a national coordination mechanism of government agencies involved in cybersecurity. The group’s responsibility is to coordinate with representatives of the private sector and state, local and territorial authorities to respond to a “significant cyber incident”. The unified coordination group consists of the heads of the agencies responsible for the country’s cyber security.



THE UNITED KINGDOM



## CYBERSECURITY COORDINATION AT THE NATIONAL LEVEL

In the UK, responsibilities for securing cyberspace at the national level are distributed as follows:

1. National Security Secretariat at the Cabinet Office – governance and policy coordination.
2. National Cyber Security Centre, part of the National Signals Intelligence Agency (GCHQ) - the main agency responsible for ensuring cybersecurity.
3. Ministry of Defense - Cyber Defense.
4. Investigatory Powers Commissioner's Office - Oversight body for GCHQ and surveillance powers more broadly.

Governmental coordination and strategic governance of cybersecurity as a whole is the responsibility of the Cabinet Office, the ministry responsible for cross-government action and direct implementation of the Prime Minister's policies. Within it, the strategic cybersecurity mandate is vested in the National Security Secretariat, which is led by the National Security Advisor. The NSS supports the National Security Council – composed of senior ministers - and the Prime Minister directly on national security matters. The intelligence and security agencies are answerable to the government through an independent mechanism called the Joint Intelligence Committee.

The operational aspects of cybersecurity are implemented by the National Cyber Security Centre (NCSC), a new body that has absorbed the roles of the Cyber and Government Security Directorate (CGSD) at the Cabinet Office. The functions of the NCSC include the provision of cybersecurity education, awareness-raising and training, collaboration with private sector representatives to exchange information and share best practices, improvement and maintenance of the UK's cybersecurity technical capabilities and operational architecture, and collaboration with law enforcement and international partners.

The NCSC is the CERT for the UK, while the National Crime Agency (a UK version of the national high-level police force similar to the FBI) has the role of combating cybercrime.

The NCSC also provides *information assurance* to the entirety of the government. As such, they are responsible for helping to secure the information and communications of every department, providing guidance and advice - for example, what software can be installed and how to monitor networks for threats. The NCSC gives direct support to some key government departments and provides a secure filtered DNS service to the public sector.

The NCSC is the public-facing part of the Government Communications Headquarters (GCHQ), the signals intelligence agency of the UK, which is far larger than intelligence bodies. GCHQ formally depends on the Foreign Office, the minister of which is legally responsible for its operations. However, they work very closely with the Cabinet Office and other departments, including the Ministry of Defence, when it comes to matters of information exchange and threat management.

The other main functions of the GCHQ in relation to cybersecurity are the detection and analysis of cyber-attacks that affect national security and provision of support to the NCA on serious cybercrime.

Oversight of the intelligence agencies is provided by a system of independent commissioners, which has been recently more centralized around the Investigatory Powers Commissioner, also responsible for countersigning surveillance warrants.

The Ministry of Defence is responsible for the UK’s military cyber defense. Its functions include the use of cyberspace for military purposes and the strengthening of defensive and offensive capabilities. The 13th Signal Regiment is the dedicated cyber defense group. GCHQ provides extensive support to the military, this being its original founding mission.

The UK has a very strong private sector working on cybersecurity, oftentimes in partnership with the government.

Critical infrastructure in the UK

The critical infrastructure of the UK consists of 13 critical sectors with individual competent authorities.

SECTOR	SECTOR RESILIENCE LEAD
Chemicals	Department for Business, Energy and Industrial Strategy
Civil nuclear	Department for Business, Energy and Industrial Strategy
Communications	Department for Culture, Media and Sport
Defence	Ministry of Defence
Emergency Services	Department of Health, Department of Transport, Department of Home Office
Energy	Department for Business, Energy and Industrial Strategy
Finance	HM Treasury
Food	Department for Environment, Food and Rural Affairs
Government	Cabinet Office
Health	Department of Health
Space	UK Space Agency
Transport	Department of Transport
Water	Department for Environment, Food and Rural Affairs

At the national level, critical infrastructure protection is the responsibility of the NCSC, which exercises this authority through critical sector regulators rather than through direct channels. Some responsibilities for support are jointly taken with the Centre for the Protection of National Infrastructure (CPNI). Critical sector entities are accountable to sector regulators, while sector regulators are accountable to the NCSC. The NCSC sets out the main framework for regulating the country’s critical infrastructure, according to which all regulators are obligated to define responsibilities for the critical sector under their competence, write down mandatory norms and ensure their implementation.

Under the Security of Network & Information Systems Regulation, adopted in 2018, which is based on the NIS Directive, critical infrastructure sectors are required to report significant cyber incidents to the NCSC within 72 hours of their occurrence. Failure to comply with this regulation, depending on the outcome of the incident, might result in a fine of up to 17 million Pounds. The amount of the fine is determined on a case-by-case basis. The fine should be proportionate to extent of the breach. Critical entities are required to provide the NCSC with information on all significant incidents that threaten the entity's security. If the incident contains signs of a criminal offence, the relevant law enforcement agency is also involved in the subsequent investigation process.

The NCSC conducts periodic audits of critical infrastructure entities. The frequency and procedures of the audit are described in a separate order and are not unplanned.



**ESTONIA**

## CYBERSECURITY COORDINATION AT THE NATIONAL LEVEL

Cyber actors in Estonia are coordinated by the Cyber Security Council of the Security Committee of the Government of Estonia, which is responsible for monitoring the implementation of the obligations under the National Cyber Security Strategy. The Council prepares an annual report on the implementation of the activities outlined in the Action Plan and submits the report to the Government.

Managing cybersecurity policy at the national level is the prerogative of the Ministry of Economy and Communications. The Estonian Information System Authority (RIA) is the Estonian information systems authority under the Ministry of Economy and Communications, which ensures the administration, coordination, development of state information systems, including cyber incident response and emergency preparedness.

The RIA is also responsible for overseeing the Estonian e-Government Platform, including the National Electronic Personal Identification Infrastructure and Data Exchange Infrastructure (X-Road). In addition, it provides Internet services to local and state agencies.

The RIA is affiliated with the Estonian Computer Security Incident Response Team (CERT-EE), which monitors and responds to cyber incidents nationwide.

In 2014, the Cyber Defense Department was established in the Ministry of Defence. Its functions are to plan, implement, and develop information security policy in the defense system.

The Estonian Cyber Defense Unit is a union of volunteers who ensure public awareness-raising of cyber threats in peacetime and help national CERT-EE during a crisis. The Unit members are not required to have specific technical skills, but knowledge and experience should be related to cybersecurity.

In early 2017, the Estonian government approved the National Defense Development Plan 2017-2026, which established a cyber-command unit within the Estonian Defense Forces. The new unit is equipped with technical and software capabilities for military cyber operations.

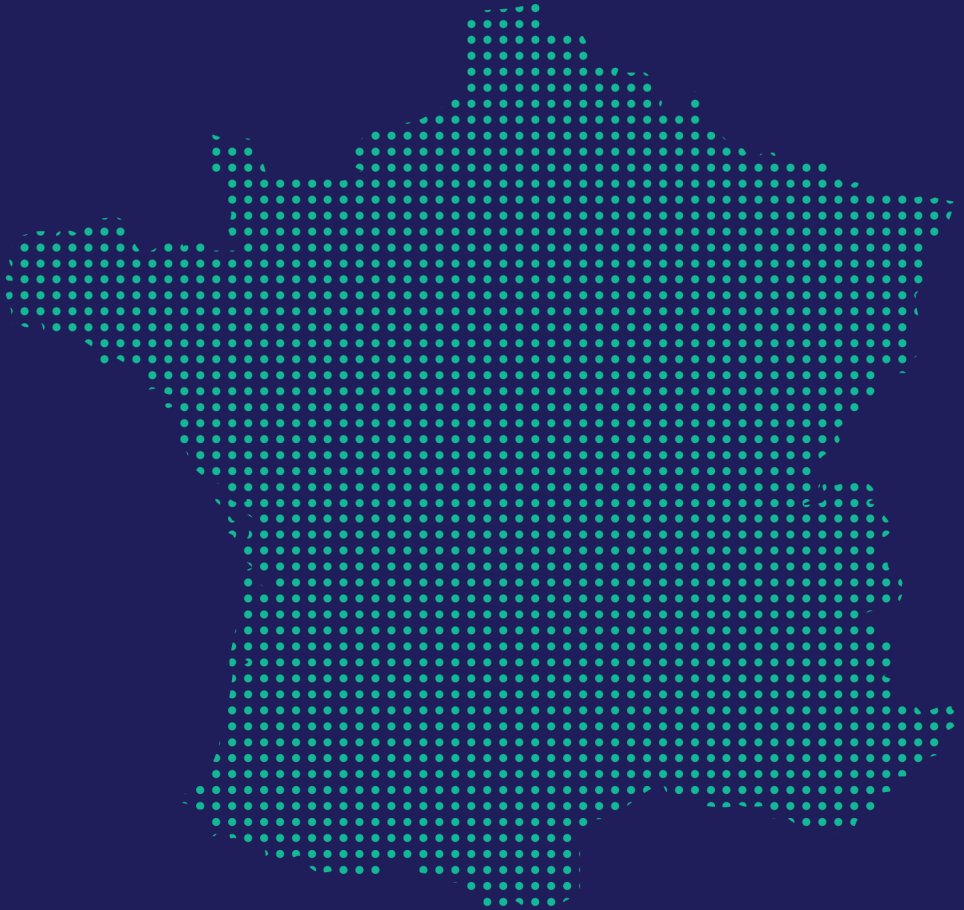
## CRITICAL INFRASTRUCTURE IN ESTONIA

The RIA directly oversees all critical sectors in Estonia, although this oversight does not include control of entities through various technical means. All critical entities are required to comply with the safety standards set by the RIA. The RIA is authorized to verify that the entity's technical facilities and information security documentation meet prescribed norms. If necessary, the RIA is also empowered to have access to the information system of a critical subject, if such access is necessary for imminent incident handling procedures.

The critical subject is obligated to inform RIA about the incidents that may affect national security or delay the delivery of the service no later than 24 hours following their occurrence. Failure to comply with the obligations set by the RIA might result in a fine of up to € 20,000.

Estonia's critical infrastructure includes the following sectors:

1. Energy and Networks: electricity, oil and gas reservoirs, transmission and distribution systems;
2. Communication and Information Technologies: telecommunications, transmission and communication systems, software, hardware and networks, including Internet infrastructure;
3. Financial system: banks, investments;
4. Healthcare: hospitals, healthcare facilities, laboratories and medicines, search, rescue and ambulance services;
5. Food: security, means of production, food industry;
6. Water supply: reservoirs, water supply and water networks
7. Transport system: airports, ports, intermediate means of transport, railway and mass transit networks, traffic management systems;
8. Production, storage and transportation of hazardous goods: chemical, biological, radiological and other hazardous materials;
9. Government agencies: critical services, government facilities, information networks providing national security and defense, resources, databases and court records, cultural assets of national importance.



FRANCE

## CYBERSECURITY COORDINATION AT THE NATIONAL LEVEL

In France, the Prime Minister is responsible for implementing cybersecurity policies and developing information system security rules. The order establishing the French National Networks and Information Security Agency (ANSSI) entrusts the Strategic Committee for Information Systems Security with the overall leadership of the French Cyber Security Policy. The Committee coordinates and implements information security measures under the auspices of the Secretary-General for Defense and National Security. In addition to the Secretary-General of Defense and National Security, the Strategic Committee consists of the representatives of the French government, such as:

- Chief of General Staff;
- Secretary-General of the Ministry of Internal Affairs;
- Secretary-General of the Ministry of Foreign Affairs;
- Director of the Defense Procurement Agency;
- Director of the Directorate of Foreign Intelligence;
- Director of Defense Information and Communication Systems;
- Director of State Information and Communication Systems;
- Director of Public Policy Modernization;
- Director of the Internal Intelligence Directorate;
- Co-Chair of the National Council for Economy, Industry, Energy and Technology;
- Director of the National Networks and Information Security Agency.

ANSSI is the organization responsible for coordinating information system security activities. It sets government e-security standards, audits critical infrastructure, and manages the Computer Incident Response Team (CERT), which is responsible for tackling cyber incidents nationwide.

Military cybersecurity is overseen by the Ministry of Defense. According to the Unified Doctrine of Cyber Defense, cyber defense planning is part of the functions of the Chief of General Staff.

## CRITICAL INFRASTRUCTURE

The ANSSI, which **reports to the Prime Minister**, is responsible for overseeing critical infrastructure sectors of France, while the sector-relevant ministry is responsible for implementing and enforcing cyber safety standards in critical entities. Ministries represent the main contacts and supervisory agencies for critical entities.

Each critical entity has an individual information security strategy and action plan. The entity is required to designate a Security Liaison Officer, who will have **access to confidential information**



**and will be in direct contact with the ANSSI.**

ANSSI conducts periodic inspection of entities through “Trust Service Providers” - organizations and individuals accredited by ANSSI. Trust Service Providers are divided into 4 areas: Cyber Security Audit Service Providers, Incident Detection Service Providers, Integration Response Service Providers, and Architecture Service Providers. All kinds of information system audits are pre-planned and agreed with the entity.

None of the French legislative acts prescribe technical supervision procedures by ANSSI. Critical entities are required to implement network monitoring tools to ensure traffic control and comply with the requirements set by the supervisory authority without the involvement of ANSSI.

Critical infrastructure is divided into 4 main areas, covering 12 critical sectors. All critical sectors have a coordinating body - the relevant ministry of the sector. The sovereignty direction includes the government sector, the security of which is the responsibility of ANSSI.

**French Critical Infrastructure Directions and Sectors**

BASIC HUMAN NEEDS	SOVEREIGN	ECONOMIC	TECHNOLOGICAL
Food	Civilian activities	Energy	Communication, technologies and broadcasting
Water management	Legal activities	Finance	Industry
Health	Military activities	Transport	Space and research



GERMANY

## CYBERSECURITY COORDINATION AT THE NATIONAL LEVEL

The Federal Office for Information Security (BSI) is Germany's main government agency providing cybersecurity at the national level. Duties of the BSI include:

- Protection of critical infrastructure;
- Ensuring cybersecurity;
- Cryptography;
- Certification of safety products;
- Accreditation of safety product testing laboratories.

BSI manages the National Cyber Incident Response Team (CERT-BUND), whose functions are to:

- Analyze and respond to cyber incidents;
- Develop recommendations for relevant agencies;
- Assist other agencies in handling cyber incidents.

BSI operates the Information Technology Information Center. The functions of the center are:

- Ensure timely reporting of cyber incidents;
- Respond to a cyber incident in coordination with CERT-BUND.
- Cyber threat assessment and public-private sector coordination in case of threat detection.

The Center is available 24/7 for federal agencies and critical service operators. The Center also monitors the networks of government and partner agencies through special sensors.

In 2017, the German government created a Cyber and Information Domain Service under the Ministry of Defense. The main function of this agency is to defend military cyber networks of Germany.

## CRITICAL INFRASTRUCTURE

In Germany, critical infrastructure includes 7 sectors: energy; information technologies and telecommunications; water; food; healthcare; finance and insurance; transport.

Security of critical infrastructure is the responsibility of BSI, which is a security-type organization accountable to the German Minister of the Interior.

The BSI has the right to request information from critical entities, analyze data, launch investigative activities, and monitor networks with technical and non-technical tools, if necessary. Such access shall be subject to the protection of corporate and personal information under applicable law. The BSI has the authority to remotely access and manage information systems of entities in emergency cases. Should the critical entity violate requirements of the BSI, the maximum amount of the administrative penalty is EUR 20 million.



## ANNEX 2: THE EUROPEAN UNION'S CYBERSECURITY FRAMEWORK

## THE NIS DIRECTIVE

In 2016, the European Parliament adopted the NIS Directive, intended to improve cybersecurity in EU member states. According to the Directive, all EU states are obligated to:

- Bring national legislation in line with the Directive;
- Identify critical service providers;
- Establish a Computer Security Incident Response Team (CSIRT);
- Establish one or more agencies responsible for national cybersecurity;
- Cooperate and establish the CSIRT network, through which information on incidents and cyber risks will be exchanged throughout the Union.

All EU countries shall identify critical sectors (transport, water supply, financial services, healthcare) and critical service providers. Critical service providers and major digital service providers are required to take appropriate security measures and provide information to the responsible authority about serious cyber incidents. It should be noted that electronic communications and service providers are not critical infrastructure entities and therefore are not covered by this Directive. Activities of these providers are regulated by the Directive 2002/21 / EC, which obliges them to provide any information (including financial) to the national regulatory authority upon request. The national regulator, in turn, is required to follow all privacy rules and explain to the service providers the purpose for which the information had been requested. This Directive does not cover cybersecurity regulations for providers. Electronic communications and service providers are also required to comply with GDPR requirements for personal data protection.

According to the Directive, all EU member states should consider the following criteria while identifying critical service providers:

- The organization (public or private) must provide services necessary for the implementation and maintenance of critical social and/or economic activities;
- Implementation of these services should depend on the network and information systems;
- In the event of an information security incident, **significant damage** should occur as a result of service disruption.

According to the same Directive, significant damage is determined taking into account the following circumstances:

- The number of customers;
- Dependence of other sectors on the given service;
- Damage that may be caused to the economic and social activities and security of the country;
- Market share of the organization;
- Geographical distribution area;
- Ability to provide alternative ways of providing services in the event of an incident.

The scheme of critical infrastructure sectors and critical service providers presented by the European Parliament includes the following areas:

SECTOR	SUBSECTOR	TYPE OF ENTITY
1. Energy	(a) Electricity	Electricity undertakings, which carry out the function of 'supply'
		Distribution system operators
		Transmission system operators
	(b) Oil	Operators of oil transmission pipelines
		Operators of oil production, refining and treatment facilities, storage and transmission
	(c) Gas	Supply undertakings
		Distribution system operators
		Transmission system operators
		Storage system operators
		Natural gas undertakings
Operators of natural gas refining and treatment facilities		
2. Transport	(a) Air transport	Air carriers
		Airport managing bodies, airports and entities operating ancillary installations contained within airports
		Traffic management control operators providing air traffic control (ATC) services
	(b) Rail transport	Infrastructure managers
		Railway undertakings, including operators of service facilities
	(c) Water transport	Inland, sea and coastal passenger and freight water transport companies, not including the individual vessels operated by those companies
		Managing bodies of ports including their port facilities and entities operating works and equipment contained within ports
		Operators of vessel traffic services
	(d) Road transport	Road authorities responsible for traffic management control
		Operators of Intelligent Transport Systems

3. Banking		Credit institutions
4. Financial market infrastructures		Operators of trading venues
		Central counterparties (CCPs)
5. Health sector	Health care settings (including hospitals and private clinics)	Healthcare providers
6. Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption but excluding distributors for whom the distribution of water for human consumption is only part of their general activity of distributing other commodities and goods, which are not considered essential services
7. Digital Infrastructure		IXP (Internet Exchange Point)
		DNS (Domain Name System) service providers
		TLD (Top-Level Domain) name registries

The NIS Directive applies to two types of organizations: critical service operators and digital service providers. Critical service operators are organizations that provide services that are important to economic well-being and normal functioning of the society. While digital service providers are organizations that operate in the field of digital services, such as online search engines, companies involved in online sales, and so-called suppliers of “cloud technologies.” The NIS Directive does not apply to digital service providers with fewer than 50 employees and/or an annual turnover of less than €10 million.

Implementation of the NIS Directive is carried out by sector-specific authorities. The responsible authority is the same as the regulatory body. A regulatory body is an agency responsible for cybersecurity of the critical sector and not the sector’s business activities.

Each critical sector has one or more regulators. In the countries represented in the study, the regulator of the government sector is the same agency that ensures cybersecurity at the national level.

The NIS Directive sets out a general framework for incident reporting and does not specify how incident reporting should be organized at the national level. There are three main models of incident reporting in EU countries:

- Critical service providers and digital service providers report significant incidents directly to the national CSIRT;
- Critical service operators and digital service providers report significant incidents to the sector regulator, which in turn provides this information to the national CSIRT;
- The hybrid model, when in one country, a part of the sectors has individual regulators and they report to said regulators, while another part of the sectors provides incident information directly to the national CSIRT.

## EU GENERAL DATA PROTECTION REGULATION (GDPR)

On May 25, 2018, the EU General Data Protection Regulation came into force. The Regulation applies to any organization, registered in the EU, that handles personal data as part of its activities. Additionally, the regulation applies to organizations that are not registered in the EU, but process the data of EU citizens.

According to this regulation, personal data processing is legal if the following requirements have been met:

- The person has consented to the processing of his or her data for one or more specific purposes;
- Processing is necessary to fulfill a contract concluded with the person, or to prepare a contract at his / her request;
- Processing is necessary for the organization to perform its statutory duties;
- Processing is necessary to protect vital interests of the person;
- Processing is necessary to exercise functions or powers conferred by law;
- Processing is necessary to protect legitimate interests of the organization or a third party.

According to the regulation, a data security breach is an incident that has resulted in accidental or unlawful destruction, loss, alteration, disclosure, or unauthorized access of personal data.



All EU member states are required to designate an agency or agencies that will be responsible for the protection of personal data. In the event of a breach, the organization shall notify this agency no later than 72 hours after the discovery of the breach.

Organizations are required to record all cases of data breaches and measures taken as a result. Organizations are also required to develop data security policies and incident detection and response plans.

Violation of the rules of the regulation is divided into two main categories: if the organization has violated its reporting obligations when a data breach was detected, and if the organization has violated the rules related to obtaining consent of a person. In the first case, maximum amount of the fine is EUR 10 million, or 2% of the annual turnover, while in the second case the maximum amount of the fine is EUR 20 million, or 4% of the annual turnover.



INSTITUTE FOR DEVELOPMENT OF FREEDOM OF INFORMATION (IDFI)

 20, T. SHEVCHENKO STREET, 108. TBILISI  + 995 32 2 92 15 14

 [info@idfi.ge](mailto:info@idfi.ge)  [www.idfi.ge](http://www.idfi.ge)