DCAF Geneva Centre for Security Sector Governance

# Georgia Cybersecurity Governance Assessment

Author
**Ms. Natalia Spînu**

November 2020

# Table of Contents

MAIN CYBERSECURITY THREATS AND NEEDS OF GEORGIA ..... 4
LEGAL FRAMEWORK AND POLICY GOVERNING CYBERSECURITY IN GEORGIA ..... 7
NATIONAL CYBERSECURITY STRATEGY OF GEORGIA ..... 8
MAIN ACTORS IN CYBERSECURITY IN GEORGIA ..... 9
NATIONAL CERT ..... 10
LINKED PROJECTS CONTRIBUTING TO STRENGTHEN THE CYBERSECURITY ECOSYSTEM IN GEORGIA ..... 11
COOPERATION AMONG CYBERSECURITY STAKEHOLDERS ..... 12
PROTECTION OF CRITICAL INFORMATION AND INFRASTRUCTURE ..... 13
CONCLUSIONS ..... 13

## The author

Ms. Natalia Spînu is a cybersecurity expert with more than 10 years of work experience in governmental and non-governmental sectors in the Republic of Moldova. She is a member of the Emerging Security Challenges Working Group which operates under the Partnership for Peace (PfP) of Defence Academies and Security Studies Institutes, as well as co-seminar leader of the Program on Cyber Security Studies from The George C Marshall European Centre for Security Studies, a program which is tailored for senior officials responsible for developing or influencing cyber legislation, policies, or practices.

Currently, Ms. Natalia Spînu is Chief of Governmental CERT in the Republic of Moldova, under her leadership CERT-GOV-MD became actively involved in many national cybersecurity development processes, including national cybersecurity program and policy developments, organizing cyber awareness conferences and workshops, building capacity for universities to prepare qualified workforce for cybersecurity sector of Moldova and others. She is responsible for strategic planning and international and intergovernmental cooperation, national cybersecurity policy, international coordination with MFA and International Projects on various tasks related to Cybersecurity.

As a cybersecurity expert, Ms. Spinu has experience and is specialized in the following areas: team and project management, ethical hacking, network security, penetration testing and security architectures, cybersecurity program and policy development, audit and implementation of business continuity (ISO-NIST) standards associated with cybersecurity and information security issues, technological risk analysis, etc.

Keywords: cybersecurity, threats, information, Georgia, national strategy, cybersecurity actors, needs, opportunities.

## Summary

This report is a two-factor analysis of cybersecurity: the legislative framework and key national actors in cybersecurity. The first part of the report presents the main cybersecurity threats in Georgia and the needs arising from national security objectives. The report describes the normative and legislative framework of Georgia covering the main aspects of information security and ensuring a level of national security of the population, while mentioning the main objectives of the national cybersecurity strategy. The second part of the report analyses the national cybersecurity strategy, the main actors within the state responsible for the national action plan for the national cybersecurity strategy in Georgia. The final part reflects upon the conclusions that have been extracted following the study and elaboration of this report.

## Acknowledgements

We would like to express our gratitude to Mr. Andro GOTSIRIDZE, Head of Security Department at Diplomat Georgia, who kindly agreed to discuss the details of the Georgian National Cyber Security initiatives and present critical issues and challenges with regards to their responsiveness to cybersecurity in Georgia. We also acknowledge his individual contributions to this report and appreciate the valuable input received. Mr. Gotsiridze's guidance and knowledge on the subject has been useful to draw a parallel between the national situation and the methods applied in addressing the cybersecurity challenges versus the impactful results obtained. Good practices and examples of different policies to address national security, gave us insights into innovative practices and perspectives to improve the current strategy and effective tools to help achieve strategic goals.

# MAIN CYBERSECURITY THREATS AND NEEDS OF GEORGIA

The steps taken by Georgia's cyber actors in the field of cybersecurity for the past decade have led to Georgia becoming among the top ten worldwide countries in the UN ITU Cyber Security Index, which measures the commitment of countries to cybersecurity at a global level. In order to calculate this Index, the study examines five main directions of cybersecurity: the legislative base; the technical equipment; the organizational structure; the development of capacities; and cooperation. Clearly, advancement in this ranking means recognition for the national cybersecurity system, and it can be noted that Georgia was assessed to be the leading country in the CIS area. Despite these successes, the strategic and conceptual documentation of cybersecurity, as well as the legislative base, requires fundamental renewal.

Georgia is one of the first countries in the world who saw the need to not only defend its land, air and sea space back in 2008, but also to protect its cyberspace from recurrent and targeted cyberattacks alongside actual military operations on its soil. Despite the progress that has been made and efforts put into countering and minimizing cyberattacks on its soil, Georgia is still required to make deep efforts at taking its cybersecurity development to an improved national-strategic level. If in previous years, a steady ground for cybersecurity was created, it is critical to continue sustainable development of these supportive frameworks, maintain existing progress and build an institutional structure that will strengthen national cybersecurity capabilities and Georgia's cybersecurity policy strategic directions.

Public sector e-services use two-factor authentication and strong cryptographic solutions in national electronic authentication. The cryptographic solution must comply with NIST Special Publication 800-78-3, ECRYPT II Yearly Report on Algorithms and Key sizes (2011-2012); with Article 14 of the Law on the "Procedure for Registering Citizens of Georgia and Aliens Residing in Georgia for Issuing Identity (Residence) Cards and Passports of a Citizen of Georgia", which defines the "e" characteristics of the ID card and its certificate requirements; with the Government Decree No. 88 on "Approval of Technical Regulation of Digital Signature Certificates and Certification Authorities Issuing Digital Signature Certificates"; Article 3, which states that qualified certificates shall comply with ETSI TR 102 437 "Guidance on TS 101 456"; and PKI applet used for cryptographic functions of ID card has algorithm RSA-2048.

There is a secure inter-organizational data exchange environment in the country (secure Internet), which enables public sector entities to provide secure web services for citizens and entrepreneurs. Private sector and other entities will be interfaces within this environment, if they provide or participate in a public service. The Georgian Government granted authorization to the Data Exchange Agency to establish and maintain the Georgian Government Gateway – a security platform for data exchange between the government and private entities. G3 – a Georgian Governmental Gateway Data Exchange infrastructure tier, enables e-ID management (registration, authentication and authorization), security, applications interoperability and e-services integration using web-based workflow for interconnection of back-office systems, providing a single integrated view of the Government by standardizing the process for submitting transactions and documents, and providing a single registration and sign-on experience.

Georgian cybersecurity achievements are not limited to the technical aspects but include organizational and legal capacities. Georgia has indeed enacted an e-friendly cybersecurity and data protection legal ecosystem. Georgia is the first Eastern Partnership

(EaP) country who is in most instances compliant with Union acquis in eGOV and ICT[1]. In 2017 Georgia fully integrated the eIDAS – Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market – and repealed Directive 1999/93/EC in its new law on Electronic Document and Electronic Trust Services, thus establishing rules and conditions for using qualified electronic signature, secure digital authentication and other qualified trust services similar to the EU requirements. The aforementioned presents a good opportunity for Georgia to initiate acknowledgement of Georgian trust services by the EU Member States and start the process of Georgia's integration into the EU Digital Single market. Comprehensive ICT legislative and regulatory frameworks addressing cybersecurity have been implemented, and legislation protecting the rights of individuals and organizations in the digital environment has been adopted in Georgia. Laws have been enacted to address the protection of critical information infrastructure (CII), the liability of ISPs, incident reporting obligations and the security of the e-transaction law of Georgia on "Electronic signatures and electronic documents"[2]. Georgia, along with other states, adopted the Uniform Electronic Transaction Act – UETA. It specifies the standards for the use of electronic digital details, but it does not oblige companies to use electronic signatures instead of written ones.

Statistical data collected by the Computer Emergency Response Team (CERT-GOV-GE) from the LEPL Data Exchange Agency of the Ministry of Justice of Georgia through the use of various technological means (network and IP monitoring system, portals, sensors etc.) makes it clear that the number of registered incidents within the period from 2014 to 2019 has at least doubled. The number of infected IP addresses has also increased, including cyber events relating to various portals.

Attempts to downgrade Georgia's progress achievements in the Euro-Atlantic integration process and marginalize its western aspirations in the eyes of European partners by diminishing Georgia's role, are among the strategic goals of the Russian Federation, which they implement by using a wide-range of methods including kinetic, hybrid or information warfare. The primary target of these threats is to establish unauthorized access to information possessed by Georgia's private and public critical infrastructures. As such, high intensity, targeted, wide-scale attacks and other threats of this nature are still seen as one of the major challenges for Georgia; addressing them is Georgia's main strategic goal.

The modern and effective use of ICTs in practice could be seen in recent years and has been affirmed to be actively used by various terrorist organizations, such as ISIS, for recruitment and propaganda purposes as well as for building a localized internal terrorist network within the country. In November 2017, a wide-scale anti-terrorist operation was carried out to neutralize one such terrorist threat. Critical infrastructure has also become an important target for terrorists – in particular ICTs which are used for carrying out and delivering functions and services critically important for the streamlined functioning of the state, the society and its citizens. Growing threats associated with cyber incidents and computer-related malfunctions related to planned attacks can cause the interruption or suspension of the functionality of vital information systems and services of critical importance. Cyber-attacks limit economic activities, may bring breakdowns to e-Governance services and bring considerable financial loss. Today, critical infrastructures in Georgia's public and private sectors are mostly using ICTs in their everyday activities. Accordingly, to discredit technologies used by them and cause losses to the

1 https://eap-csf.eu/wp-content/uploads/EaP-Index-2017.pdf
2 https://matsne.gov.ge/ru/document/download/20866/4/en/pdf

interests of state, business or individual customers is a goal of many organized crime groups. Furthermore, today losses will be much higher than they were in 2008 because of the increased reliance of public and private sectors on ICTs. Taking into consideration the above-mentioned reasons and the existing reality, where critical information systems and service provider subjects do not possess even a minimal required level for provisioning proper information and cybersecurity, it is a strategic-level issue for Georgia's cybersecurity to elevate protection and security standards for critical information infrastructures administrated by public and private sectors.

## Cybercrime in Georgia

Cyberspace is a fertile ground for committing criminal acts. Thanks to technological innovations, the possibility to commit crime remotely and stealthily, the evidence variability, difficulties in identifying criminals and jurisdiction related problems make the unsanctioned use of Internet a space favourable for cybercriminals. The "cyber" element is becoming an indivisible part of almost any type of crime[3]. Georgia has defined cybercrimes and established them with a legislation in line with the Council of the Europe Convention on Cybercrime; the Georgian Legal Framework on cybercrime covers all offences, as required by the Convention on Cybercrime. Georgian cyber-crime legislation is in line with the European principles and rules both in terms of substantive and procedural aspects, namely the national law, criminals' illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, offences related to child pornography, and offences related to infringements of copyright and related rights[4].

It has been observed over the period of the last five years that cybercriminals have increased attacks on state-owned critical sectors and other commercial sector services, and aim to cause at least reputational loss and even, with proper conditions, achieve total shut down of the mentioned sector. A good example of such a case is a DDoS attack carried out in 2016 against the banking sector and state financial e-Services. As a result, the functionality of online banking services and state tax systems were, at least for a short period of time, halted. The most prevalent attacks against critical infrastructures that have happened in recent years are: phishing, ransomware, deface, DDoS, and email spoofing[5].

[3] cybercrimes (i.e. fraud, crimes against property, online drug trade etc...) and represents crime auxiliary factor. In the "classical" sense, there has been seen an increase in crimes committed against computer data and system confidentiality, availability and integrity. Today, types of cybercrime including unauthorized access to computer systems, unlawful possession of computer data, data infringement, unauthorized use of computer equipment, crimes relating to child pornography and violation of intellectual property are widely prevalent. Especially significant forms of cybercrime can be found in the form of phishing, identity theft, and use of malware and deface.

[4] https://matsne.gov.ge/en/document/view/16426?publication=209

[5] https://csis-website-prod.s3.amazonaws.com/s3fs-public/201218_Significant_Cyber_Events.pdf

# LEGAL FRAMEWORK AND POLICY GOVERNING CYBERSECURITY IN GEORGIA

## National Laws and strategy on Cybersecurity

The key law that sets the ground for information and cybersecurity frameworks is the Information Security Act of Georgia[6]. The law is supplemented by a number of sub-normative acts that define and further develop the legal provisions for practical implementation. Despite an existing legal framework, the cybersecurity legislation has a few gaps requiring relevant consideration from the respective authorities. Namely, there is an urgent need to develop an inclusive framework for the classification of critical information infrastructure assets which include the private sector. The methodology and principles for identifying those critical information infrastructures should be conducted in conformity with the Directive on security of network and information systems (NIS Directive) and available EU best practice. There are many steps to follow for developing strong enforcement mechanisms to ensure Critical Information System Subjects' (CISS) compliance with the new legal regime of cybersecurity. The lack of cybersecurity safeguards for CISS is a challenge in terms of the availability, integrity and confidentiality of critical information systems and services. In addition, the existing legal framework does not provide for incident reporting and vulnerability disclosure rules and procedures. Incident taxonomy rules and response schemes are also missing; there is no central registry of national-level cybersecurity incidents.

The law defines the Data Exchange Agency and the Cybersecurity Bureau of the Ministry of Defense (MoD) as the government agencies responsible for the country's cybersecurity. Under the Criminal Code of Georgia, unauthorized access to computer information; creation, utilization or distribution of malware; and the exploitation of network systems are considered crimes, as is cyber-terrorism. On the international level, Georgia ratified in 2012 the Convention on Cybercrime, which was developed by the Council of Europe. Georgia now shares the common governing principles of the Convention's member states and aims to create a comprehensive legal foundation on the national level while strengthening international cooperation.

The Public Administration Reform Action Plan 2019-2020 adopted by Government Decree N. 274 of June 10th, 2019, directly highlights government efforts undertaken for the cyber protection of critical information networks and infrastructures: "In order to ensure the high standard of governance, the high level of safety and security of critical information infrastructures and information systems are also very important. New action plan defines the activities, which will ensure the safety and security of such systems and in general, will raise the awareness regarding the cyber and information security." (Chapter 4, Public Administration Reform Action Plan 2019-2020). In particular, it includes the following activities: the development of a methodology for defining the critical information system subjects, the implementation of intrusion detection system in the public sector, the creation of a curricula for cyber hygiene in schools, and relevant updated training materials for the e-learning platform (https://elearning.dea.gov.ge/).

6 https://matsne.gov.ge/en/document/view/1679424?publication=3

## International Agreements

The EU-Georgia Association Agreement (2017-2020) aims to strengthen the Georgian public institutions' cybersecurity capacity. The Association Agenda between the European Union and Georgia[7] (2.6. Economic Development and Market Opportunities, sub-part: Cooperation in the Field of Digital Economy and Society) refers to "efforts to increase the cyber resilience of key critical infrastructure sectors and public sector organizations, drawing from relevant EU experiences and in line with EU norms". It is expected that this Twinning project will cover all priorities stipulated in the Agenda, in particular the following Union acquis:

- EU External Cyber Capacity Building Guidelines – Council Conclusions and Operational Guidance.
- Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).
- Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 as regards managing risks by digital service providers posed to the security of network and information systems and determining a substantial impact of incident.

# NATIONAL CYBERSECURITY STRATEGY OF GEORGIA

Georgia's first cybersecurity strategy and action plan was developed in 2013. This 2013-2015 document defines Georgian government policy on cybersecurity, reflecting the strategic goals and main principles as well as establishing action plans. The primary strategy goal is cooperation among state, private and international organizations. The cybersecurity strategy involves five essential elements: research and analysis, a legal foundation, coordination on an institutional level, raising public awareness with outreach and education, and international cooperation. Georgia's cybersecurity strategy for 2017–2018 improved public awareness and established an education base as key directions for cybersecurity in Georgia and outlined concrete actions to achieve these objectives. A national program for raising cybersecurity awareness is yet to be established, as currently cybersecurity awareness-raising efforts are sporadic and not supported by dedicated budgetary allocations. The absence of a coordinating structure during 2018-19 is probably one of the reasons why Georgia, unfortunately, entered 2020 without a National Cybersecurity Strategy. However, the country is already working on a third-generation strategy that is positively perceived by the international community and cyber-experts, which places it in leading positions in international ratings.

This third national cybersecurity strategy still under development, and currently in a draft state, is also important because it is bringing together concrete components aimed at improving not only the country's cyber and information security environment, but also strengthening capabilities to combat cybercrime and effectively make the use of cyber defence techniques. In most cases, it is difficult to set a boundary, as the steps taken towards improving Georgia's cyberspace equally serve the development of a cyber-defence environment and, at the same time, effective cybercrime neutralization.

Georgia shall set goals to make achieved results even steadier, and in response to new threats will turn its cyber and information security environment into a more secure do-

[7] https://eeas.europa.eu/sites/eeas/files/annex_ii_-_eu-georgia_association_agenda_text.pdf

main. All this is achievable by active engagement and cooperation of both public and private sectors, and academic circles, and by using approaches of complex nature. Having taken into consideration all these factors, in order to timely and effectively counter threats and incidents coming from cyberspace, the present strategy sets a goal to bolster cyber culture and cyber education when it comes to cyber defence and cybercrime, to make the governance system more sustainable, to strengthen public-private partnership, to establish strong human resources and promote Georgia as a safe and secure country at the international level.

The Georgian National Cybersecurity Strategy and Action Plan 2020-2022 is expected to be adopted early 2021. Key components of the strategy are interrelated with the twinning project as regards to public-private cooperation in the field of critical information infrastructure protection, awareness raising, capacity building of key stakeholders and affected industry representatives, and the building of a sustainable and well-functioning institutional-organizational framework for better cybersecurity in the country. The main part of the draft document focuses on goals, objectives and activities: (1) Bolster the development of cyber-culture among information society and organizations to support resilience to threats and incidents in cyberspace; (2) Sustainability of a cybersecurity governance system and enhancement of the public-private cooperation; (3) Strengthen cyber capabilities and development of a strong cyber workforce; (4) Strengthen Georgia's position as a net contributor to international cybersecurity at an international scale.

# MAIN ACTORS IN CYBERSECURITY IN GEORGIA

Cybersecurity became a state priority after the 2008 Russia-Georgia war, when the country experienced a wide-scale cyberattack on its governmental as well as banking and media sectors. In 2010, the LEPL Data Exchange Agency under the governance of the Ministry of Justice of Georgia was established, with one of its very functions to protect and support information and cybersecurity of critical infrastructures. In the following years, several organizational structures equipped with the authority to deal with cybersecurity and cybercrime have been formed:

## LEPL Cybersecurity Bureau of the Ministry of Defence of Georgia

The Cyber Security Bureau (CSB) is a Legal Entity of Public Law (LEPL) under the Ministry of Defence (MoD) created in 2014 as a result of strong governmental commitment to strengthening the cybersecurity dimension within the defence sphere. The mission of the Bureau is to establish and develop a robust and reliable information security system which will minimize harmful consequences of any cyber-attack and/or computer security incident and will allow rapid ICT restoration.

The fundamental principle and mandate of this organization encompasses security of the CISS (Critical Information System Subject) of the defence domain plus initiation of the different ICT standards. At the initial stage of development, in conjunction with the NATO allies and partners, the CSB elaborated its first Cybersecurity Policy, clearly indicating its core functions and targeted areas. Due to the complexity of the issue, the CSB continues the process of sophistication by strengthening areas, ranging from strategy development, legal and human capacity to technological advancement. As for the technicalities to detect and prevent cybersecurity incidents, the Computer Security Incident Response Team (CSIRT) of the CSB conducts proactive and reactive services on a daily basis, as well as digital forensics, malware analyses, IT audits, live response and threat hunting.

## LEPL Operative-Technical Agency under the State Security Service of Georgia

After the structural reforms of 2015, the State Security Service of Georgia (SSSG) was established as an independent entity and is vested with the power to acquire, process and collect information regarding threats to national security. The activities of the SSSG are focused on the identification, prevention and deterrence of potential threats, as well as to carry out relevant measures to fully protect the State's national interests and the safety of each citizen. The LEPL Operative Technical Agency (OTA) is under the supervision of the SSSG, also accountable to the Prime Minister, and guarantees the conduct of covert investigative activities and electronic surveillance measures when addressed by the relevant investigative, intelligence and counterintelligence agencies equipped with the appeal, in line with the respective legislative procedures and norms.

## Division to fight against cybercrime within the Main Division of Organized Crime and Central Criminal Police of the Ministry of Internal Affairs of Georgia

The Ministry of Internal Affairs (MIA) of Georgia is responsible for cybercrime law enforcement. This activity has been carried out by the Cyber Crime Division (CCD) under the Central Criminal Police Department (CCPD) since December 2012. The MIA has also established a Special Sub-unit for Computer-Digital Forensics within the Forensics-Criminalistics Main Division; this sub-unit is the first handler of digital forensic evidence. Georgia is part of the Council of Europe/Budapest Convention and carries out cybercrime law enforcement functions in accordance with EU and CoE standards. The National Security Council of Georgia (NSC) is an eight-member advisory body responsible for national security policy planning and coordination. The Office of the NSC is responsible for cybersecurity inter-agency coordination and cooperation, as well as supervision over policy and strategy development process.

# NATIONAL CERT

The Computer Emergency Response Team (CERT-GOV-GE), a subsidiary unit of LEPL Data Exchange Agency in the Ministry of Justice of Georgia, has signed a considerable number of memorandums of cooperation to share knowledge and experience with respective organizations of European and Eastern Partnership countries (i.e., Lithuania, Romania, Moldova, Ukraine, Belarus). Georgia is actively participating in international Cyber Exercises (CyberEXE) and study programs, where the country constantly takes leading places in terms of observed results.

Difficulties remain in replicating existing cybersecurity endeavours at large scale due to a lack of affordable training programs and educational opportunities. Despite the developments made, lack of trained personnel is a common problem[8]. The need to train professionals in cybersecurity has been recognized by the Government and has been documented in the cybersecurity strategy of Georgia. Within public institutions, the training in cybersecurity, both for IT and general staff, is very limited and very low numbers of public servants have undergone it. Cybersecurity awareness and cyber-consciousness are often absent in the mind-set of employees in the government sector. Private sector offers for cybersecurity training are also limited to non-existent. A high demand for cy-

[8] https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B

bersecurity certification is almost exclusively serviced through the invitation of instructors from abroad or through online programs.

# LINKED PROJECTS CONTRIBUTING TO STRENGTHEN THE CYBERSECURITY ECOSYSTEM IN GEORGIA

In the recent years, a number of projects have been contributing (including with the support of international donors and partners) to strengthen the cybersecurity ecosystem in Georgia. A Memorandum of Understanding (MoU) on Cybersecurity Cooperation between the Government of Georgia and the Government of the United Kingdom was signed in 2019 and aims to further develop long-term and large-scale cooperation in the field of cybersecurity. Under the umbrella of this MoU, the Cybersecurity Capacity Review was conducted by the Global Cyber Security Capacity Centre (GCSCC)[9], the third National Cybersecurity Strategy Development process has started and discussions among stakeholders on the identification of critical information infrastructures have commenced. Recommendations from the review were thoroughly reflected in the National Cybersecurity Strategy development process. UNDP, USAID, NATO (HQ and Liaison Office), GIZ, other international donors and local partners have been helping the DEA and cyber authorities to perform systematic and ongoing awareness-raising and training activities during the last five years to build up cyber professionalism and proficiency.

Implementation of the new regional program 'EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries'[10] contributes to improving the cyber-resilience and criminal justice response of EaP countries. The program has two key building blocks: first, the development of technical and cooperation mechanisms increasing cybersecurity and preparedness against cyber-attacks; second, the full implementation of an effective framework to combat cybercrime, including substantive and procedural criminal legislation, law enforcement and judicial authorities' capacity to investigate, prosecute and adjudicate cases of cybercrime, measures to enable international cooperation, and cooperation between public authorities and private entities. The Council of Europe/Budapest Convention continues to provide the benchmark for an effective framework.

The twinning project "Promote the strengthening of E-Governance in Georgia (E-Government Georgia)", from 2012-2014. The overall objective of the project was to build the capacity of the Georgian Public Administration in the implementation of reforms and democracy for the benefit of its people by using ICT. The project's purpose was to strengthen the capacities of the Data Exchange Agency and to consequently implement the best and most suitable e-policies in Georgia based on EU practice.

"Support to the Public Administration in Georgia"- EU funded, from 2019-2021. The objective of the project is to improve the efficiency, accessibility, accountability and transparency of the Georgian Public Administration in accordance with European principles of public administration and best practices. More specifically, the project is mainly focused on improving the results-based approach in policy planning, development, coordination, monitoring and evaluation, increasing the awareness of civil servants and streamlining the implementation of civil service reform in public institutions, improv-

9 https://www.oxfordmartin.ox.ac.uk/cyber-security/

10 https://eufordigital.eu/discover-eu/eu4digital-improving-cyber-resilience-in-the-eastern-partnership-countries/

ing the intra and inter-ministerial business processes related to policy making and service delivery enhancement, thus impacting the efficiency of the administration and the quality of service delivery. The project aims to strengthen policy development and the implementation of anti-corruption and transparency national policies, thus increasing the accessibility, accountability and transparency of the executive branch, combating corruption, and establishing an efficient, accountable and transparent institutional and legal framework for timely and reliably delivered public and electronic services. Finally, the project aims to raise public awareness and increase visibility of the Government's public administration reform agenda as well as of available public services.

Twinning project "Capacity Building of the Civil Service Bureau of Georgia to Implement the Civil Service Reform" - EU funded, from 2018-2020. The objective of the project is to enhance the professionalism of civil service in Georgia. More specifically, the project aims to strengthen the institutional and human resources (HR) capacities of the Civil Service Bureau in managing the implementation of the Civil Service Reform, through the reinforcement of the legal framework, introduction of modern Human Resource Management (HRM) information system, tools and techniques, development of training scheme for HR managers, and improvement of the Assets Declaration Monitoring system.

"Facility for the implementation of the Association Agreement in Georgia" - EU funded since February 2019 to 2021 (phase II of the aforementioned project has been launched). The project provided assistance to the DEA through expert mission to support the identification of relevant and important aspects of the NIS Directive to be taken into consideration during the approximation process and Twinning project preparation stage.

# COOPERATION AMONGST CYBERSECURITY STAKEHOLDERS

The high rate of private ownership of critical information systems in Georgia makes close collaboration between private infrastructure operators and government security stakeholders crucial. Despite this, exchange of information between domestic stakeholders stays formally unregulated. This is largely due to the fact that the Law on Information Security identifies only public institutions as Critical Information System Subjects (CISS) and therefore, the private organizations, including Internet Service Providers (ISPs), are not obliged to cooperate or report on cybersecurity incidents.

The adoption of legislative requirements for the exchange of information between public and private sectors and between public institutions has been high on the agenda since the establishment of the first cybersecurity framework. The objectives of such cooperation included the information exchange on cybersecurity incidents, mutual assistance, and the management of cyber crises in a coordinated manner.

At this stage, the Governmental CERT regularly exchanges information with the Central Criminal Police Department on cyber incidents which include a cybercrime element. The State Security Agency is also involved in this information exchange process in case cybersecurity incident becomes a matter of national security, as the cooperation of ISPs and law enforcement agencies is governed by a Memorandum of Understanding. By signing the agreement, the ten largest ISPs, the Prosecutor's Office and the Ministry of Internal Affairs (MIA) have agreed on the rights and responsibilities of the parties involved in the process of investigation.

# PROTECTION OF CRITICAL INFORMATION AND INFRASTRUCTURE

Georgia's Law on Information Security mandates the identification of a narrow set of Critical Information System Subjects (CISS) under government control. According to this Law, entities were selected on the basis of "the severity and scope of the expected results of the information system malfunction; the severity of economic damage for the subjects and/or the State; the necessity for information system services for smooth functioning of the state defence; the number of information system users; material status of a subject and the amount of expected expenses incurred as a result of imposing relevant obligations on the subject".

The protection of the CISS is ensured in several steps:

- The Law makes incident reporting to CERT.GOV.GE compulsory for all general public sector organizations and to CSIRT.MOD.GOV.GE for Defence critical infrastructure.
- The Law obligates CISS to develop internal rules for information security that meet minimum security standards defined by the DEA in a separate normative act. Upon year three in the implementation of these rules, mandatory annual audits are conducted by the DEA or a DEA-authorized organization to evaluate these policies for compliance. The recommendations of the audit reports are legally binding.
- The CISS are subject to mandatory penetration testing and a vulnerability assessment carried out by the DEA.
- Where audits or testing reveals non-compliance with an organization's information security policy, the CISS are required to investigate the causes and eliminate shortcomings. However, no enforcement mechanism exists in case of not following these recommendations.
- The CISS shall designate an information security manager tasked with providing assessment of information assets, monitoring compliance with information security policy and reporting on its implementation.
- Besides the information security manager, the CISS are obliged to appoint a cybersecurity specialist responsible for the monitoring of computer systems, the detection, reporting, and analysis of cyber incidents, and to coordinate with CERT.GOV.GE.
- The DEA and the CSB have set up net flow sensors and network firewalls for each respective CISS to assist in the detection and analysis of cyber incidents.

# CONCLUSIONS

Georgia is a developing European country with enormous potential. Unfortunately, one of the defining steps in strengthening cybersecurity laws and regulations came only after the state fell victim to a cyber-war. Paradoxically, we came to understand the need for a cybersecurity policy and strategy only after we faced large-scale attacks. Assistance from other GUAM member countries in the region strengthening the national security of critical infrastructure has in recent years fostered the implementation of an impressive set of projects and platforms to automate sensitive processes, regulate important data and invest optimal resources to train environmental employees, for the public and the ICT domain to be ready to respond to possible cyber-attacks. There were assumptions about the repetition of a state cyber-attack in 2019, which was investigated and con-

firmed by CERT Georgia in February 2020 – but this fact was kept confidential from the media, especially regarding the details of the attack scenario and the victims.

At present, Georgia has one of the strongest supports in the field of cybersecurity. New policies and strategies are planned for the next period, as well as information and training sessions for cybersecurity specialists, and the third security strategy is being developed covering areas that were omitted in previous versions, so that the current version is harmonized with European legislation and security standards in the field.

Georgia is one of the few countries where cybersecurity development has been ahead of its ICT development. From a cybersecurity point of view, the situation is very good. Analysing other developing countries undertaking similar EU projects in the region such as Moldova, Armenia, Azerbaijan and Ukraine, it is clear that Georgia has the most advanced and supported frameworks in the field of cybersecurity, and is offering opportunities to share experience and good practices with other states in the region to ensure a digital environment for a better future in the cyber field.

DCAF Geneva Centre for Security Sector Governance

DCAF Geneva Headquarters

P.O.Box 1360
CH-1211 Geneva 1
Switzerland

info@dcaf.ch
+41 (0) 22 730 9400

**www.dcaf.ch**

@DCAF_Geneva