Cybersecurity Capacity Building in Georgia: Examining Georgia-EU Cooperation in Countering Cyber Threats

Georgian Foundation for Strategic and International Studies

LEPOIX Manelle
June 2023

Direct descendant of Arès, Greek God of war, – Phobos - terror incarnate, inspires fear. He is depicted furiously, striding along, wearing a lion's skin and Medusa's head on his shield. Phobos is the very embodiment of a frosty, paralyzing feeling. The cyber-threat is just as chilling, a branch of warfare, if not a direct descendant of it, and in itself personifies the fragility of the computer systems that make up our world and support our governments. The paralysis of our IT systems is far from being a mere metaphor. In Georgia, Phobos is everywhere. The Russian Federation, Arès, is broadcasting its son as a threat to its neighbor. In 2019, Georgia suffered a large-scale attack[1]. Websites, government agencies, state bodies, courts, universities, and television channels were all affected, on an unprecedented scale. The Russian attacker[2] remains somewhere, present, threatening, always ready to destabilize Georgia. This is all the more true given that Georgia had already taken steps to secure its cyber-network, since 2010 (annex 1). The Russian Federation is making its presence felt, even as Georgia tries to break out of its grip. Russian cybercrime groups are even well known: DarkSide, Evil Corps, Revil... [3]Insecurity is constant. The main challenge, apart from securing government networks, remains the sensitive link with sovereignty. Regarding sovereignty as a "general rule", the rule no. 4 of the Tallinn 2.0 Manual[4] considers that any intrusion that causes physical damage or loss of functionality to the systems under attack represents an attack on sovereignty. The French approach is also along these lines, since "any unauthorized penetration"[5] into the digital spheres of the state represents a violation of a country's sovereignty. According to the European Union, cybersecurity "covers the activities necessary to protect networks and information systems as well as the users of these systems and other persons exposed to cyber threats"[6]. Overall, we can easily say that today, a huge proportion of our data is online. The dematerialization of all our administrative documents is palpable. Government websites, the very embodiment of the state, are under cyber-threat. Cyber-attacks are attacks that occur in cyberspace, which is the global, interconnected network of information and communication infrastructures, including the Internet, telecommunications networks, computer systems and all the information they contain[7]. Cyber-attacks can be defensive or offensive. They are therefore the "use of cyber

[1] Przemyslaw Roguski, Russian Cyber Attacks against Georgia, Public attributions and sovereignty in Cyberspace, in Just Security. 06/03/2020.
https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

[2] Przemyslaw Roguski, Russian Cyber Attacks against Georgia, Public attributions and sovereignty in Cyberspace, in Just Security. 06/03/2020.
https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

[3] Tielidze Giorgi, Russia's changed attack tactics and vectors in cyberspace, Georgian Foundation for Strategic and International studies, Expert Opinion n°171, 14p. 2021.
https://gfsis.org.ge/publications/view-opinion-paper/171

[4] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Centre of Excellence, Tallinn Manuel on the International law applicable to cyber warfare, Cambridge University Press. 282p. 2013.
https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

[5] Ministère des Armées, Droit International appliqué aux opérations dans le cyberespace. 18p.
https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqué%20aux%20opérations%20dans%20le%20cyberespace.pdf

[6] European Council, Council of the European Union, Cybersecurity: how the EU tackles cyber threats. Last reviewed on 24/05/2023.
https://www.consilium.europa.eu/en/policies/cybersecurity/

[7] Rabussier Camille, L'application du droit international dans le cyberespace, Université Paris II Panthéon Assas, 102p. 2019.
https://idc.u-paris2.fr/sites/default/files/memoires/Mémoire%20Camille%20Rabussier%20Application%20du%20droit%20international%20dans%20le%20cyberespace.pdf

capabilities with the primary aim of achieving objectives in or through cyberspace".[8] The daily lives of thousands of users are online[9], as are government networks. Cyber-attacks are increasingly used in times of war, as demonstrated by the war situation in Ukraine[10]. However, Russia is also using these cyber-attacks to keep a firm grip on the region, a constant reminder of its presence. As well as destabilizing opponents, the cases are often linked to cyber espionage[11].

Russian-Georgian relations are tense. Georgia is at a key moment: the choice between freeing itself from Russian domination and joining the European Union or clinging to the Russian yoke. The enemy is subversive. At the same time, the European Union is becoming aware of the importance of its action in cyberspace, in view of its growing importance[12]. Both countries are aware of the danger this represents, as well as the need to repel the enemy. The priorities that concerned the EU & Georgia are set out in several successive agreements or directives (annex n°2). The main ones are:

- Association agreement (2014).
- NIS Directive (2016).
- Eastern Partnership, post-2020 objectives (2020).

The stakes are high. There is even a desire to extend the benefits of the EU's Digital Single Market to Georgia, in order to develop the digital economy, bring economic growth and generate employment[13]. The security of this market is essential, especially given the attacks on Georgia. The aforementioned agreements and directives will be the pillars of this paper. Without ignoring the other projects underway or completed, we will analyze the results of this cooperation over almost 10 years in terms of cyber security. We will look in more detail at what these agreements and directives mean in practical terms for Georgia. This paper will therefore cover a relatively broad period, from 2014 to the present day, in order also to offer a long-term vision of the challenges post-2023. We will consequently look at the objectives of European-Georgian cooperation in the field of cyber-security, once again emphasizing the importance of this area both for Georgia and for Europe's ambitions. The issues surrounding cyber-security in Georgian-European relations are crucial. Firstly, Georgia is at a crossroads: continuing its alignment with European positions remains a choice, which may prove key for the future. Secondly, it is also a question of internal security, which is being reinforced by the war unleashed by Russia in Ukraine. Indeed, any form of interference in Georgian affairs could be decisive. The outcome of the war remains more than uncertain. Russia's presence in Georgian cyberspace could prove to be a potential first step for Russia in the case of a Ukrainian defeat.

---

[8] International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manuel on the International law applicable to cyber warfare, Cambridge University Press. 282p. 2013. https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

[9] 77.4% of the population aged 6 years and older has used the Internet within the last 3 months. GeoStat, National Statistics Office of Georgia, Indicators of using information and communication technologies in the households, 2021. 11p. https://www.geostat.ge/media/40378/Indicators-of-Using-ICT-in-Households---2021.pdf

[10] Think Tank Russia's war on Ukraine: Timeline of cyber-attacks. 21/06/2022. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

[11] Cybersecurity & infrastructure security agency, America's cyber defense agency, Russia Cyber Threat Overview and Advisories. https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia#:~:text=The%20Russian%20government%20engages%20in,harm%20regional%20and%20international%20adversaries.

[12] European Council, Council of the EU, Cybersecurity: how the EU tackles cyber threats, last reviewed on 24 May 2023. https://www.consilium.europa.eu/en/policies/cybersecurity/

[13] EU4Digital, Georgia https://eufordigital.eu/countries/georgia/ : EU4Digital identifies the main obstacles in cyber security areas of member of the EaP, to building resilience in member countries.

Russian interference therefore remains a dangerous and ever-present threat in the Georgian landscape. Finally, aligning with European positions remains a rather positive option for Georgia, especially in view of a potential spill-over[14], and even more so in the current context. This is all the more true given that Georgia has already suffered several Russian cyber-attacks. Georgia and the European Union seem to want to align around a common objective: to secure cyberspace in order, among other things, to repel adversaries. For Georgia, securing cyberspace also means securing its sovereignty, and therefore its land space. It is therefore essential to observe whether these numerous efforts have been successful. It is also necessary to analyze these advances in order to foresee the future, the next challenges that Georgia could face. Overall, Georgia's efforts in the field of cyber-security are also an opportunity to question its candidate status, which will - or will not - be announced next October. Alignment with European priorities makes sense in this general context. If we take a close look at the twelve priorities, there are two points that could be closely or remotely related to cyber security. Point 2 focuses on guaranteeing the functioning of state institutions and point 6 is based on the fight against organized crime[15].Thus, we can legitimately ask ourselves **to what extent has European-Georgian cooperation on cyber security been effective over the last ten years**? It will, therefore, be question of an analysis of European ambitions in terms of cyber security (I), the Georgian situation and its needs (II), and finally an analysis of the results obtained over the last ten years (III). To measure the effectiveness of European-Georgian cooperation, it is important first to observe the provisions of the agreement, with regard to European and Georgian needs. Similarly, effectiveness will be measured by the improvement - or otherwise - of cyber security in Georgia, but also by the improvement of relations between these two areas. Analysis of future challenges and forecasts will also enable us to draw conclusions about effectiveness.

I- European ambitions regarding cyber-security.

In May 2010, the European Union announced its Digital Agenda for Europe, marking the first concrete targets for cyber security. Europe's ambitions are high, as can be seen from the desire to create the Digital Single Market. The European Union has become aware of the intensification of the digital network and the growing importance of cyberspace in general. In this sense, the European Union has grasped the need to protect this space as well, while taking into account the need to extend this protection to its partners. We will begin by taking stock of the situation in the European Union (a), before looking at its objectives (b). Finally, we will look at the three directives and agreements mentioned above in order to understand what is at stake (c).

a) The current situation within the EU regarding cyber-security.

The European Union currently has a legislative package on cyber security[16]. This has been built up over several years.

In June 2016, the Council issued its first report, which agreed the next steps in the fight against criminal activities in cyberspace. Also in 2016, the Directive on the Security of Network and Systems (NIS) was introduced. This is the first legislative measure taken at European level

---

[14] Haas B Ernst, Beyond the Nation-State: Functionalism and International Organization, Stanford University Press, 584p. 1964.

[15] EEAS Europa, The Twelve Priorities.
https://www.eeas.europa.eu/sites/default/files/documents/12%20Priorities.pdf

[16] Arthur Olivier, Cyber sécurité : que fait l'Union européenne, in Toute l'Europe, 09.01.2023.
https://www.touteleurope.eu/economie-et-social/cybersecurite-que-fait-l-union-europeenne/

to step up cooperation between Member States on cyber security issues. The directive provides, for the strengthening of national cyber security capabilities, the establishment of a framework for voluntary cooperation between Member States through the creation of a "cooperation group" and a "European network". It is meant to facilitate the sharing of technical information on risks and vulnerabilities. The directive also defines, in order to strengthen the cyber security of essential service operators' national cyber security, rules with which these operators must comply, as well as an obligation to notify each incident that has had an impact on the continuity of essential services. Finally, common European rules for digital service providers have been introduced[17]. Georgia, in particular, has been able to comply with this directive[18].
However, it is in April 2018 that the Council adopted the cyber-security regulation, which provides for a Europe-wide certification system and a European cyber-security agency to succeed the European agency responsible for information network security[19]. In May 2018, the Council became able to impose sanctions, as it established a framework enabling the European Union to impose targeted restrictive measures to deter or counter cyber-attacks against the European Union and its Member States[20]. It is now possible to impose sanctions on persons or entities responsible for cyber-attacks or attempts. The European Union may also provide financial, technical, or material support to third States or international organizations (in accordance with the requirements of the CFSP[21]). The European Union is therefore continuing its efforts to pass on the benefits of the Digital Single Market to its partner countries, particularly those in the Eastern Partnership[22].

In December 2020, the European Commission and the European External Action Service presented a new cyber security strategy to strengthen Europe's resilience. The idea is, among other things, to protect itself against cyber threats and to establish a secure communications environment. In March 2021, the Council adopted conclusions on the cyber security strategy, underlining the importance of this area in building a resilient, green, and digital Europe. The aim is to achieve strategic autonomy and make the European Union a digital leader.

In order to strengthen cyber security and resilience on a European scale, the EU will draw up an agreement on the NIS 2 Directive. The Council and Parliament have reached a provisional agreement on measures to ensure a common high level of cyber security across the Union. It is also with a view to improving the incident response capacity of the public and private sectors within the Union. The directive entails new legislation to ensure that risk and incident management are strengthened, while at the same time extending cooperation within

---

[17] ANSSI (Agence nationale de la sécurité des systèmes d'informations), adoption de la directive NIS : l'ANSSI, pilote de la transposition en France. 2016.
https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

[18] The European Union for Georgia, Strengthening Cybersecurity capacities in Georgia.
https://eu4georgia.eu/projects/eu-project-page/?id=1458

[19] ENISA, European Union Agency for Cybersecurity. Established in 2004, ENISA has been strengthened by the EU Cybersecurity Act.
https://www.enisa.europa.eu/about-enisa

[20] European Union External Action, EU imposes first ever cyber sanctions to protect itself from cyber-attacks. 30/07/2020.
https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en

[21] Council Decision, decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States. 30/07/2020.
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1127

[22] European Council, Council of the EU, Cybersecurity: how the EU tackles cyber threats, last reviewed on 24 May 2023.
https://www.consilium.europa.eu/en/policies/cybersecurity/

the scope of the rule[23]. New rules have been put in place: risk management measurement basis, reporting obligations, harmonization of the rule. The Council adopted the conclusions of the cyber security strategy in March 2021. All this information once again shows that the European Union considers cyber security to be a pillar in the construction of its future, since the aim is to increase the ability to make autonomous choices, always with a view to strengthening digital leadership[24].

In conclusion, this brief overview shows that the European Union is very active in its will to secure its network, particularly in view of the potential cyber-attacks that could disrupt it. Similarly, it is seeking to create a secure digital marketplace, as we have already mentioned. Finally, more generally, the European Union wishes to become a digital leader. To achieve this, the cooperation with partners, in particular with the Eastern Partnership, is key. Overall, the European Union has specific objectives in terms of cyber security.

b) European ambitions regarding the cyber security field.

Europe's cyber security strategy has developed considerably over the last few decades. The aim here is to provide a brief overview of the future developments envisaged by the European Union, so as to grasp its main ambitions. As we have already mentioned, the Digital Single Market almost single-handedly indicates Europe's ambitions, but several other projects have been announced.

Firstly, as mentioned, the NIS 2 directive will see its measures implemented from 18 October, the date on which the NIS directive will be repealed. Among other things, the NIS 2 Directive extends the measures taken by NIS to new sectors, increasing the number concerned from 19 to 35. It also removes the distinction between operators of essential services and providers of digital services, provides a minimum list of basic security elements to be applied by businesses. Lastly, it strengthens the role of the cooperation group in drawing up strategic policy decisions.[25] Clearly, we can see that the European Union is seeking, as a logical extension, to broaden the scope of its action. Data protection is given even greater prominence, as is the prevention of cyber-attacks. Similarly, the European Union is still taking into account the threats of paralysis of its organizations, as well as cyber espionage. The sectors concerned include banking systems, research infrastructures and financial markets. A strong European Union means securing its network and protecting it against potential destabilization. Also, the European Union would like to set up a Cybersecurity Industrial Technological and Research Centre through national coordination, in order to increase its autonomy[26].

Secondly, in its Digital Europe program, the European Union is promoting cyber resilience to ensure online security[27]. The European Commission and the High Representative

---

[23] European Council, Council of the EU, Strengthening EU-wide cybersecurity and resilience- provisional agreement by the Council and the European Parliament.
https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/
[24] European Council, Council of the EU, Cybersecurity: how the EU tackles cyber threats.
https://www.consilium.europa.eu/fr/policies/cybersecurity/
[25] Cyber Risk GmbH, The NIS 2 Directive
https://www.nis-2-directive.com/
[26] Akhvlediani Tinatin, Digital and Cyber dimensions of the EU association agreements with Georgia, Moldova and Ukraine, 15p. December 2019.
[27] European Commission, Cybersecurity policies
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

have responded to the growing number of cyber-attacks and new challenges in the post-covid world by announcing the Cyber Security Strategy[28]. The strategy is based on strengthening all the European tools for technological sovereignty. One of the points on which the European Union is focusing on is the intensification of its cooperation with partners who share the values of democracy, the rule of law and human rights. In short, the aim is for the 4 cyber-communities (internal market, law enforcement, diplomacy, and defense) to work closely together, to raise awareness of the threats[29]. In addition, the ambition is also to react quickly to these threats. In the long term, the goal is to guarantee a global and open Internet with solid guarantees in the event of risks to the security and fundamental rights of Europe's citizens.
To finish, the Cyber Solidarity Act proposed by the Commission on 18 April 2023 is a step in this direction[30]. Once again, this is support for the construction of a digital Europe as a whole. The European cyber shield will be made up of security operation centers, and the law aims to improve the detection of cyber threats.

Thus, the European ambitions in the field of cyber security are more than clear: Digital Europe will be massive and will take into account Europe in the broadest sense, not just the European Union. It wants to become a leader in digital technology, without neglecting its partners. Clearly, the European Union is aware of the importance of supporting and integrating countries such as Georgia. Therefore, the European Union wants to strengthen its collective capacity to respond to cyber-attacks, while at the same time promoting international cooperation to guarantee international stability in the cyberspace. A great deal of investment and innovation is on the way, based on the projects outlined over the past two years, and the Digital Europe program (2021-2027) provides for €1.9. billions of investments in cybersecurity.

c) Extensions outside the European Union.

As we mentioned, the European objective is to extend its benefits to the whole of Europe, not just the European Union. For example, in 2021, the European Union provided essential hardware and software worth $231,000 to the Cyber Security Office of the Georgian Ministry of Defence as a technological solution to protect information systems against cyber threats. Thanks to the EUSAFE program, the technologies and financial resources could be sufficient, even without human capital, to improve Georgian capabilities in this area. The EUSAFE project aims to equip IT infrastructures and cyber security technologies with cutting-edge technology. This will improve detection of infected systems, minimize incidents of unauthorized access and reduce data loss[31]. The European objective is therefore to create a safer environment for cyber security systems. The European Union is therefore active, including in third countries. Georgia is at the heart of a fruitful environment for strengthening the cyber security ecosystem. There are several European projects, including the SAFE EU4 security accountability and fight against crime in Georgia program, which aims to fight crimes, cyber and hybrid threats. There is also EU4Digital, which aims to improve resilience (in the Eastern Partnership countries) by

---

[28] European Commission, The Cybersecurity Strategy
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
[29] The European Union has three instruments at its disposal to do so: resilience, technological sovereignty, and leadership; the operational capacity to prevent, deter and intervene; and cooperation to promote a global and open cyber space. Investment in the digital transition is part of the 2020-2025 Strategy for the EU.
[30] European Commission, The EU Cyber Solidarity Act.
https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity
[31] Delegation of the European Union to Georgia, The European Union supports cyber security bureau through advanced technological capacities to enhance cybersecurity in Georgia, 30/06/2021.
https://www.eeas.europa.eu/delegations/georgia/european-union-supports-cyber-security-bureau-through-advanced-technological_en

enhancing cyber-resilience and the judicial response to crime. Two key blocks are mentioned: technical development and cooperation mechanisms to increase cybersecurity and preparedness against cyber-attacks, as well as, through law enforcement and judicial authorities, the ability to investigate, act and cooperate internationally. The European Union wants to combat cyber threats by fighting organized crime through the CFSP framework. To this end, the EU has even listed cybercrime as one of its top 10 priorities for 2018-2021.

Six priorities were identified in 2014 and updated in 2018: developing defense capabilities, protecting the European Union's communication and information networks, improving educational exercises, technological research, increasing civil-military cooperation and focusing on international cooperation. We can see that the European Union is determined to expand beyond its borders. For Georgia, cooperation remains key. [32] As far as our subject is concerned, we are going to focus on three major agreements reached by the European Union, and from which Georgia benefits. The first is the Association Agreement (2014), followed by the NIS Directive (2016), and finally the Eastern Partnership (focusing on Georgia), without ignoring other projects.

Firstly, chapter 8 article 324 of the Association Agreement demonstrates that cooperation in the field of information society is one of the most important areas of cooperation[33]. It covers the exchange of information and the improvement of security networks for online public services.[34]Overall, the Association Agreement aims to improve cooperation in defense and security policy, strengthen bilateral dialogue and facilitate Georgia's participation in the CSDP. The European Union has therefore put in place several tools and programs to assist Georgia's resilience and capacity to deal with hybrid threats[35]. The Association Agreement has little to do with the digital and cyber dimension, although it does define the scope of cooperation in the digital sectors, both in the body of the text and in the annexes[36]. In short, the Association Agreement provides the starting point for cooperation in this area, but there are no binding commitments[37]. This includes cooperation to prevent crime and illegal activities (art 17-g). Cybercrime is not directly mentioned here. However, we can assume that cyber-crime is part of illegal activities and organized crime. This is all the more true when you consider that Russian cyber-attacks could be the work of organized crime. [38] There is also a question of high-level cooperation on data protection, linked to Article 118(2), which implies that each party must adopt safeguards to protect confidentiality and individual and fundamental rights and freedoms, especially when transferring data. Finally, article 325-8 explains that cooperation

---

[32] Akhvlediani Tinatin, Digital and Cyber dimensions of the EU association agreements with Georgia, Moldova and Ukraine, 15p. December 2019.

[33] To be noted: increasing cyber security implied also protecting economic sector, another field the AA takes into account.

[34] To be more precise, it tackles electronic communications, information society, exchange of best practices and implementation of the basis for cooperation and dialogues.

[35] European Commission, Strengthening Cybersecurity capacities in Georgia, 48p.
https://um.fi/documents/385176/0/Strengthening+Cybersecurity+Capacities+in+Georgia.pdf/58a7bd7d-e7bd-af0b-8f61-d7da4428f2c9?t=1582806899150

[36] Akhvlediani Tinatin, Digital and cyber dimensions of the EU association agreements with Georgia, Moldova and Ukraine. 17p. 12/12/2019.
https://3dcftas.eu/publications/digital-and-cyber-dimensions-of-the-eu-association-agreements-with-georgia-moldova-and-ukraine

[37] European Parliament, Association agreement between the EY and Georgia- European Implementation Assessment (update), 67p. April 2020.
https://www.europarl.europa.eu/RegData/etudes/STUD/2020/642820/EPRS_STU(2020)642820_EN.pdf

[38] Tielidze Giorgi, Russia's changed attack tactics and vectors in cyberspace, Georgian foundation for strategic and international studies, Expert Opinion n°171, 14p. 2021.
https://gfsis.org.ge/publications/view-opinion-paper/171

covers the exchange of information, the improvement of security networks, the desire to obtain a comprehensive regulatory framework for electronic communications, and the strengthening of administrative capacities. Clearly, there is no direct question of cyber security. However, the Association Agreement does promote cooperation, including in cyber space sectors. Through this framework, cooperation can therefore bear fruit and be strengthened[39].

Secondly, The Association Agreement promotes cooperation. Thanks to this, Georgia was able to accede to the European NIS Directive (2016). The Directive aims to strengthen Georgia's cyber security capabilities by enhancing Georgian preparedness and resilience to cyber threats and attacks. The initial aim of the directive was to increase cyber resilience across the European Union through regulatory measures, in order to strengthen national cyber security capabilities, embed cyber security in the DNA of organizations and improve cooperation between Member States[40]. The NIS Directive is therefore not initially formulated for third countries. It is a European directive valid for Member States, and for those states, such as Georgia, that agrees to be bound by it. The alignment of Georgian security systems with European models, and in particular the NIS Directive, is reflected in the Georgia Cyber Security Strategy and action plan 2017-2018[41].The expected results of the NIS Directive in Georgia are to strengthen the Georgian model in terms of institutional governance of cyber security (revising legislation to meet European standards, developing and supporting cyber governance), strengthening the operational and technical legal frameworks to protect critical information infrastructures (improving Georgian capacity to manage cyber incidents, strengthening the cyber workforce); strengthening the national authorities' operational capacity in cyber security, and solidifying cyber culture and awareness.[42] This is the first compulsory legislation designed to increase the overall level of security in European cyberspace.
Of course, this is reinforced by other projects, such as the Twinning Project on cyber security. The aim is to create a cyber security framework, in line with the European approach, standards and policy framework. In practical terms, this means supporting Georgia in improving its institutional capabilities in the field of cyber security, enhancing the skills of its personnel and promoting close international and national cooperation. Strengthening the legal and institutional frameworks for cyber security should increase the level of security of Georgian networks, so that they are able to react to cyber-attacks.

Thirdly, EU4digital has created the Cybersecurity Guidelines for the Eastern Partnership countries (June 2020). The aim of this partnership is to strengthen cooperation between the six countries and the European Union. Several sectors are targeted, including cyber security. EU4Digitial identifies the main obstacles in cyber security areas to strengthen resilience in each country[43]. The key priorities of the Eastern Partnership are to strengthen the protection of infrastructure criteria, to solidify public-private cooperation and international cooperation in

[39] Official Journal of the EU, Association Agreement between the EU and the EAEC and their Member States, of the one part, and Georgia, of the other part. 261/4- 261/743. 30/08/2014.
https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:22014A0830(02)
[40] Scheelen Yannick, Machilsen Koen, Deprez Andy, How to prepare for the NIS2 Directive? On EY. 16/05/2023.
https://www.ey.com/en_be/cybersecurity/how-to-prepare-for-the-nis2-directive
[41] Spinu Natalia, Georgia Cybersecurity, governance assessment, Geneva Centre for security Sector Governance, 14p. November 2020.
https://www.dcaf.ch/sites/default/files/publications/documents/GeorgiaCybersecurityGovernanceAssessment.pdf
[42] The European Union for Georgia, Strengthening Cybersecurity Capacities in Georgia.
https://eu4georgia.eu/projects/eu-project-page/?id=1458
[43] EU4Digital, Cybersecurity guidelines for the Eastern Partner countries, 37p. June 2020.
https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf

cyber security, and finally, to develop the capacity to respond to cyber incidents[44]. Before looking at the details, it is important to note that Georgia was the most advanced of the six countries in terms of cyber security.

Thus, the European Union is seeking to build a secure and reliable communications network, which means it needs to export itself. It is even a European priority. Clearly, Georgia is one of the countries benefiting from this cooperation...

In conclusion, cyber security has become one of the major challenges facing the European Union in recent years, but Europe's ambitions are high[45]. Cooperation with third countries remains essential to achieve these objectives. Georgia is one of the countries cooperating in cyber security. It is therefore necessary to analyze Georgia's needs, always with a view to analyzing the effectiveness of the Georgia-EU cyber security partnership.

II- Georgia and cyber security.

As we have already mentioned, Georgia is facing numerous cyber-attacks, particularly from Russia. In 2010, Russian cyber-attacks were already being considered and described as a threat in official documents.[46] Globally, all sectors can be affected. Georgia was one of the first Eastern Partnership countries to understand the need to protect its land, sea, and cyber space. In recent years, cybercriminals have stepped up their attacks on so-called "critical" sectors (CIS), particularly those belonging to the state, and other services in the commercial sector, with the aim of damaging the targeted sector. An attack in 2016 targeted the state's online banking and financial sector, causing these services to malfunction. [47] Incidents and attacks doubled between 2014 and 2019, to prevent Euro-Atlantic integration and marginalize Western aspirations in the eyes of European partners. The main objective of Russian attacks is to establish unauthorized access to information held by private and public critical infrastructures[48]. These threats remain Georgia's main challenge. The international community supports the country[49]. Over the last few decades, the Georgian cyber ecosystem has evolved within government. In 2017, International Telecommunication Union ranked Georgia eighth out of 165 countries in terms of cyber security readiness (16th in 2014). The government has adopted a holistic approach to the building blocks of cyber security: developing a strategy, implementing the legal framework, increasing cyber competence, establishing a public-private partnership based on trust and developing international partnerships. Georgia has therefore taken cyber security into account in its legal and strategic documents (a). Nevertheless, the country faces

---

[44] European Commission, Strengthening Cybersecurity in Georgia. 48p.
https://um.fi/documents/385176/0/Strengthening+Cybersecurity+Capacities+in+Georgia.pdf/58a7bd7d-e7bd-af0b-8f61-d7da4428f2c9?t=1582806899150

[45] Also because the threat landscape “has become increasingly volatile”.
World Economic Forum, Global Cybersecurity outlook 2023, Insight report, 36p. January 2023.
https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

[46] Ministry of Defense, Threat Assessment for 2010-2013.
https://mod.gov.ge/uploads/2018/pdf/TAD-ENG.pdf

[47] Spinu Natalia, Georgia Cybersecurity, governance assessment, DCAF Geneva Centre for Security Sector Governance.15p. November 2020.

[48] The list has been established by an ordonnance made by the government of Georgia in 2014. It tackles 39 organizations: administrative bodies, Parliament, administration of the President, Tbilisi City Hall, National Bank of Georgia,…

[49] Reuters, UK announces support to protect Georgia against Russian cyber-attacks, 29/06/2022.
https://www.reuters.com/technology/uk-announces-support-protect-georgia-against-russian-cyber-attacks-2022-06-29/

other challenges and needs (b). European cooperation has, however, enabled a change in its strategy and legal framework (c).

a) The current situation in Georgia.

Georgia currently ranks 55th in the world and 30th in Europe in the Cyber Security Index (2020). Overall, Georgia scored very well on the legal aspect, and less well on the organizational aspect.[50] The country is also a signatory to the Budapest Convention. Nevertheless, Georgia has put in place several strategic and legal plans to improve its cyber capabilities.

The first national cyber security strategy was drawn up in 2013[51]. The main objective was cooperation between State, private and international organizations. Other objectives include a legal basis, institutional coordination, raising public awareness through education, and international cooperation[52]. The National Cyber Security Strategy 2017-2018 improves public awareness and establishes an educational base, outlining comprehensive actions to achieve specific objectives. For example, a national cyber security awareness program is to be set up (despite the difficulties in carrying out this project due to the lack of budget allocation)[53]. It defines the key political priorities for developing the cyber security field. The 2019-2020 plan, adopted by government decree, emphasizes the importance of cyber data protection. This plan defines the activities that guarantee the security of systems, raises awareness of cyber security, and secures information. It also aims to create an intrusion detection system.
Georgia aspires to closer relations with the European Union, also in terms of cyber security. The country has therefore complied with the NIS Directive to establish targeted and innovative cyber security. Of course, the government assumes responsibility for the security and privacy of its citizens in cyberspace, but more reliable measures need to be taken. Overall, European cooperation projects remain essential for the strategic updating of national cyber security policy.

Georgian advances are not just technical. It has put in place a legal ecosystem favorable to data protection. Indeed, the country also has a legal framework. For example, in 2017, Georgia incorporated the eIDAS regulation in line with European requirements. This protects the rights of individuals and may enable Georgia's integration into the European digital market. Another example is the Law on Information Security[54]. The overall framework is aligned with the NIS Directive, giving importance to the principles of identifying critical information infrastructures, which include the private sector. The “law aims to promote the efficient and effective maintenance of information security, define rights and responsibilities for public and

---

[50] Agenda GE, Georgia ranks 55th in the world, 30th in Europe for cyber security, 1/07/2021. https://agenda.ge/en/news/2021/1800

[51] Cyber Security Strategy of Georgia, 2012-2015. 12p. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Georgia_2012_National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf

[52] The UNDP, USAID, NATO, GIZ and other international donors have helped the cyber authorities to carry out systematic and joint awareness-raising activities in the field of cybernetics. UN also (UNOPS) delivered the essential cybersecurity equipment, training of personnel and global expertise in procurement, project management and security to improve technical and institutional capacity.

[53] Spinu Natalia, Georgia Cybersecurity, governance assessment, DCAF Geneva Centre for Security Sector Governance.15p. November 2020.

[54] The law defines the need to apply information security rules to critical information systems. This law protects the State, and legal persons essential to the defense and economic security of the State.

private sectors in the field of information security maintenance, and identify the mechanisms for exercising state control over the implementation of information security policy".[55]

Georgia also has several key players in cyber security. In 2010, the Data Exchange Agency (LEPL)[56] was created under the aegis of the Ministry of Justice. The aim of this body is to protect and support critical infrastructure information. Over time, several organizational structures have been developed: Cybersecurity Bureau (2014), which follows the Ministry of Defence's desire to strengthen the cybersecurity dimension in the defence sphere. The aim of this Bureau is to establish and develop a reliable and robust information security system that will minimize the consequences of a cyber-attack, while enabling rapid restoration of affected areas. The CSB also takes into account the Critical Information System Subject. The Bureau has developed its first cyber security policy with NATO allies and partners. Its field of action extends from the development of strategies to technological progress, without neglecting legal and human capabilities. To detect and prevent cyber security incidents, CSB's Computer Security Incident Response Team provides reactive promote knowledge-sharing with organizations in European and Eastern countries[57]. Also, since 2012, there has been a CyberCrime unit operating with the MIA, which aims to suppress, detect and prevent illegal activities committed in Georgian cyberspace. Other organizations are also involved in cyber security: the State Security Service of Georgia produces reports, the National Bank of Georgia ensures that minimum information is provided on the security standards implemented by commercial banks, etc.[58] Also, Georgia has two major cyber security bodies: CERT.GIV.GE[59] (subject to Data Exchange Agency), and GRENA[60] (research and educational networking association).
To finish, Georgia has also taken some initiatives, for example, by helping universities to have a cyber security program, or by organizing trainings at the national level, even if private companies don't put in place this kind of trainings.

In conclusion, several institutional and state bodies have been set up, demonstrating that cyber security is being taken into consideration. For the most part, these bodies meet European requirements. In terms of technology and organization, Georgia has several structures in place to promote cyber security. Nevertheless, Georgia's needs remain wide-ranging.

b) Georgian's needs.

---

[55] Legislative Herald of Georgia, Law of Georgia on Information security, consolidated versions 2015-2020 https://matsne.gov.ge/en/document/view/1679424?publication=3

[56] Legislative Herald of Georgia, On the Establishment of the Legal Entity Under Public Law (LEPL) Called the Data Exchange Agency, consolidated versions 2012-2017.
Aims to put in place the minimum requirements and suggestions in information systems (regulating and overseeing implementations).
https://matsne.gov.ge/en/document/view/89662?publication=1

[57] Spinu Natalia, Georgia Cybersecurity, governance assessment, DCAF Geneva Centre for Security Sector Governance.15p. November 2020.

[58] Akhvlediani Tinatin, Digital and cyber dimensions of the EU association agreements with Georgia, Moldova and Ukraine. 17p. 12/12/2019.
https://3dcftas.eu/publications/digital-and-cyber-dimensions-of-the-eu-association-agreements-with-georgia-moldova-and-ukraine

[59] In response to the large-scale Russian cyber-attacks in 2008, which affected government agencies and the media and damaged infrastructure, Georgia created a roadmap and framework for its cyber security strategy to manage incidents and information in cyberspace (CERT.GOV.GE, 2011), while at the same time strengthening its legislative framework (2012).

[60] Georgian Research and Educational Networking Association,
https://www.grena.ge/eng

Through the new National Strategy, we can perceive Georgia's current and future needs in terms of cyber security. In this sense, looking at the effectiveness of the European-Georgian partnership[61] will also involve analyzing the conformity of needs with the policies promoted by the European-Georgian partnership.

Cyber-attacks are on the rise. The Ministry of Defence wants to automate, digitize, and unify its activities. Centralized control systems are being introduced, enabling the effective development of communications models, but this means being even more prey to cyber-attacks. To this end, Georgia has shared its cyber security objectives for 2024. The three main pillars are: human capital, sustainable technology, and the institutionalization of processes. Georgia's first priority is to develop a skilled workforce[62]. To achieve this, it needs adequate equipment and financial resources (funds allocated by the LEPL, Cyber Security Bureau). However, it is the most vulnerable component. At present, Georgia does not have enough human capital, let alone trained human capital. The primary objective is therefore to increase educational activities and raise awareness, especially when users of cyberspace are the most vulnerable. Secondly, Georgia needs to improve its technical skills, especially when its opponent is constantly changing tactics[63]. It is essential for Georgia to equip itself with cyber specialists with solid skills in order to introduce best practice. Then, there is a need to institutionalize processes and increase effective governance. This involves opting for governance through risk-based planning, which would strengthen the country's defense capabilities. It would be possible to plan for all possible scenarios in the case of an attack. The introduction of a security standard is also key for the government. Research is then needed to identify the weaknesses. Finally, Georgia wants to ensure that its technology is sustainable in the face of increasing digitalization, which means introducing new technologies and equipping itself with the appropriate resources. Obviously, a large cyber defense budget is needed to meet these objectives. Nevertheless, the country already has some important resources to meet these requirements, such as intra agency cooperation and the Cyber Security Bureau. National and international cooperation[64] (NATO, EU) are also key sources of support[65]. Clearly, the focus is on developing an information society and cyberculture within organizations, having a resilient and cumulative cyber security governance system with a strengthened private-public partnership, and improving cybercapacity through a robust workforce[66]. The two main threats continue to be cyber warfare/information warfare/cyber espionage/cyber-attacks on state actors/cybercrime and attacks on critical infrastructures. As far as cyber-warfare is concerned, Russia is using

[61] To be noted: Georgia participates in the European Union's CSDP, as well as the SAFE Program, which provides resources for combating crime, border management, cyber security, and protection of civil society, damage to nature, etc. It is in fact a "global package" of measures taken to help Georgia. 183 million euros have been mobilized to provide practical support for the country (health, civil society, environment, etc.).
Consilium Europa, Facts and Figures about EU-Georgia Relations, 3p.
https://www.consilium.europa.eu/media/44400/685-annex-5-d-georgia-factsheet.pdf

[62] EU4Digital, Strengthening cyber-security expertise in Georgia, 30/07/2019
https://eufordigital.eu/strengthening-cyber-security-expertise-in-georgia/

[63] J.Smith David, Russian Cyber Strategy and the War Against Georgia, Atlantic Council, in Focus Quarterly, 17/01/2014.
https://www.atlanticcouncil.org/%20blogs/natosource/russian-cyber-policy-and-the-war-against-georgia/

[64] Memorandum of Understanding on Cyber Security cooperation between the government of Georgia and the government of UK (2019) in order to develop long term et large scale cooperation in cyber security, for example. Agreement with Turkey, Armenia, Lithuania, Estonia, Ukraine…

[65] Cyber Security Bureau, Cyber Security Strategy of the Ministry of Defence of Georgia 2021-2024, 15p.
https://mod.gov.ge/uploads/Cyber_Security/Cyber_Security_Strategy_of_the_Ministry_of_Defence_of_Georgia_2021-2024%E2%80%9C.pdf

[66] Civil Georgia, Georgia adopts cybersecurity strategy for 2021-2024, 07/10/2021.
https://civil.ge/archives/446772

propaganda and disinformation against Georgia. Regarding cybercrime, a document lists the dangers of cybercrime (dangerous emails, etc). It should also be noted that the National Action Plan for Georgia 2019-2021 shows that Georgia is still committed to be in line with the EU NIS Directive. For the Strategy 2020-2028, Georgia still wants a national framework in line with the Euro-Atlantic expectations. Also, twinning projects on public-private cooperation in the area of critical information infrastructure protection are needed. The establishment of a sustainable institutional and organizational framework is essential. This is all the more true when you consider that no critical information infrastructure is designated in the private sector[67]. It is essential to integrate the private sector.

The Georgian objectives are thus to support the development of cyber security within the information society of organizations in order to promote resilience in the face of incidents and threats, ensure the stability of cyber security governance systems, while improving cooperation between the public and private sectors. It is also necessary to strengthen cyberspatialities and develop a strong workforce, while reinforcing Georgia's position as a net contributor internationally. Despite the fact that organizations have made considerable progress in terms of operational capacity, the problems regarding coordination and the creation of personal & informal network remain. There is no specific budget allocated to cyber security (just funds for the Data Exchange Agency), not all sectors have been equally involved in the efforts (private sector, civil society, etc).[68] Thus, the European Union is one of the providers regarding cyber security. The main challenges remain: the lack of resources allocated to cyber security, the lack of commitment on the part of national authorities in certain areas of cyber security, the lack of awareness, the lack of qualified personnel and adequate resources. The next step is therefore to strengthen the existing legislative framework[69]. Cooperation mechanisms, defining essential services, etc. remain crucial steps[70]. However, European cooperation appears to be active.

c) Collaboration with the European Union.

As mentioned above, several projects with the European Union are in place. The projects set up with the European Union often have the main aim of promoting the strengthening of e-governance in Georgia (building the capacity of the Georgian public administration, implementing reforms to benefit the population). The goal is to improve accessibility, accountability and transparency, while complying with European principles. The objective, here, is to look at the precise objectives, before analyzing the results.

Firstly, the EU-Georgia Association Agreement aims to strengthen Georgian public institutions and their capacities. To achieve this, Twinning Projects[71] have been set up, covering

[67] Cooperation in these sectors is important: many private companies have critical information systems in Georgia. The Law on Information Security only identifies public institutions as subjects of critical information systems. Thus, private companies have no obligation to cooperate, and therefore no obligation to report cyber incidents. The adoption of legislative requirements for the exchange of information between these sectors is key (exchange of information, mutual assistance, coordinated management of cyber risks, etc.).
[68] European Commission, Strengthening CyberSecurity Capacities in Georgia, 48p. https://um.fi/documents/385176/0/Strengthening+Cybersecurity+Capacities+in+Georgia.pdf/58a7bd7d-e7bd-af0b-8f61-d7da4428f2c9?t=1582806899150
[69] There are still some problems with this law: lack of cooperation between the public and private sectors, no legal framework for certain activities, and no support for groups working on cyber incidents.
[70] European Commission, Strengthening Cybersecurity in Georgia. 48p. https://um.fi/documents/385176/0/Strengthening+Cybersecurity+Capacities+in+Georgia.pdf/58a7bd7d-e7bd-af0b-8f61-d7da4428f2c9?t=1582806899150
[71] European Commission, Strengthening Cybersecurity Capacities in Georgia, 48p.

the following priorities[72]. Overall, Georgia is following the operational guidelines and conclusions of the Council, but also the Directives of the Parliament. Finally, the Commission has put in place regulations on the digital risk of information systems and mechanisms for determining the substantive impact of an incident. Another example of cooperation could be EU SAFE (2019)[73]. It is a project to "support the advancement of technical capabilities to ensure human security". Actually, this project is part of the European Union's wider initiative for the security sector in Georgia. The aim is to help the Georgian government to achieve effectiveness and efficiency, while ensuring the accountability of security sector institutions by identifying specific needs, supplying hardware and software, and so on. Once again, the European Union wants to ensure the protection of critical infrastructures and cyber infrastructures. Both the European Union and Georgia stand to gain: the European Union appears to be a leader, capable of providing security beyond its digital market, and Georgia gains in protection. The idea is to strengthen human and technical capacities in the security sector, in line with Georgian needs. To achieve this, we need a legislative framework that forces institutions to work together according to the same European rules, thereby protecting human rights, citizens' personal data and the rule of law.

Secondly, the Eastern Partnership also includes cyber security, in view of the increase in cyber-attacks, cyber threats and cyber espionage. It aims to get involved in a number of areas: cyber security legislation, ensuring that minimum requirements are introduced in partner countries, ensuring the proper functioning of critical information infrastructures, National Risk Assessment, Reporting Mechanism/Incident Management, cooperation mechanisms, data protection, cyber security culture, cybercrime, etc. Six priorities emerged during the EaP Summit in Riga in 2015[74]. Several areas are targeted: electronic communications, infrastructures, Trust and Security, ETrade, digital skills, ICT innovations, EHealth etc[75]. To this end, the European Union has set up several projects to support these areas, such as EaP Connect (2015)[76]. According to the 2020 amendments, Georgia could benefit from this addition, particularly in view of the measures it is taking to relate to the fundamental pillars of

---

https://um.fi/documents/385176/0/Strengthening+Cybersecurity+Capacities+in+Georgia.pdf/58a7bd7d-e7bd-af0b-8f61-d7da4428f2c9?t=1582806899150
The aim is to strengthen Georgia's Cyber Security Capacities, solidifying its ability to be prepared and its resilience in the face of cyber threats. Georgian stakeholders must also be able to create a secure cyber security framework, in line with European approaches, standards and policy/legal frameworks. The specific objective is to strengthen cyber security in Georgia, with regard to the legal and institutional frameworks for increasing the security of information systems and their level of prevention, reaction and resilience. This project is in line with the NIS directive and the European guideline

[72] Twinning project "Capacity building of the Civil Service Bureau of Georgia". The aim is to implement the civil service reform, financed by the EU in 2018, until 2020. The aim is to improve the professionalism of the civil service in Georgia, in particular by strengthening institutional and human resources capacities. All this has an impact, albeit indirect, on cyber security, which needs a solid organization.

[73] Delegation of the EU to Georgia, The EU supports Cyber Security Bureau through advanced technological capacities to enhance cybersecurity in Georgia. 30/06/2021.
https://www.eeas.europa.eu/delegations/georgia/european-union-supports-cyber-security-bureau-through-advanced-technological_en

[74] Concilium Europa, Joint Declaration of the Eastern Partnership (Riga, 21-22 May 2015). 13p.
https://www.consilium.europa.eu/media/21526/riga-declaration-220515-final.pdf

[75] Akhvlediani Tinatin, Digital and cyber dimensions of the EU association agreements with Georgia, Moldova and Ukraine. 17p. 12/12/2019.
https://3dcftas.eu/publications/digital-and-cyber-dimensions-of-the-eu-association-agreements-with-georgia-moldova-and-ukraine

[76] EaP Connect.
https://eapconnect.eu/

European legislation[77]. In any case, Georgia has the shortest list of commitments to meet, as the country is the furthest ahead of European recommendations. The aim is to increase resilience and the protection in critical infrastructure information in key sectors (economy, public administration, businesses,…). The Eastern Partnership's recommendations for all six countries include legislative changes (writing National Strategy documents), having a responsible entity, establishing a methodology for identifying IICs, etc. The Eastern Partnership's recommendations for all six countries include legislative changes (writing National Strategy documents), having a responsible entity, establishing a methodology for identifying IICs, etc[78]. To support these changes, related projects are being set up, such as Cyber East (Action on Cybercrime for Cyber Resilience in the Eastern Partnership Region). Overall, these include support for cooperation between CSIRTs and law enforcement, judicial exercises on cybercrime and e-evidence, creation of a Cyber Barometer on cybercrime and cyber security, workshops on Standard operating procedures for criminal justice authorities etc[79]. The project has been extended until 2023, enabling it to obtain new resources to reinforce its actions. The "EU4Digital: Improving Cyber Resilience in the Eastern Partnership Countries"[80] program is also helping to improve cyber resilience and the justice response in the EaP member countries. There are two main strands: the development of technical cooperation mechanisms to strengthen cyber security, and preparedness for cyber-attacks. The second area is based on the implementation of an effective framework for combating cybercrime (criminal and procedural legislation, capacity of law enforcement and judicial authorities to investigate, international and public-private cooperation, etc.). Finally, as mentioned, Georgia also integrated European directive regarding cyber security, such as the NIS Directive[81]. This directive imposes many requirements on capabilities and capacities of Georgia (definition, creation and operations of policies, procedures, and structures necessary). Indeed, a technical and operational framework is needed to develop the protection of Critical Information Infrastructure. The legal, operational, and technical architecture of cyber security in Georgia is in line with European requirements. Georgia, therefore, needs to have technical support to find out the key constituencies, and needs to review its regulation.

Georgia is involved in a number of European projects aimed at strengthening the cyber sector. However, given the country's current needs and situation, as described above, it is necessary to question the effectiveness of these measures. Effectiveness will be measured by two indicators: firstly, have the links with the EU been strengthened overall, and secondly, do the results obtained by these projects correspond to Georgian needs?

---

[77] Akhvkediani Tinatin, The New Eastern Partnership- what's in it for Georgia? 11/06/2020.
https://gip.ge/the-new-eastern-partnership-whats-in-it-for-georgia/

[78] EU4Digital, Cybersecurity guideline for the EaP, 46p. June 2020
https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf

[79] CyberEast, Fact Sheet, 1p. March 2022.
https://rm.coe.int/cybereast-factsheet-march22/1680a5cc24

[80] Spinu Natalia, Georgia Cybersecurity- Governance Assessment, DCAF, Genova Centre for Security sector governance, 15p. November 2020.
https://www.dcaf.ch/sites/default/files/publications/documents/GeorgiaCybersecurityGovernanceAssessment.pdf

[81] As a reminder, NIS Directive imposed: adoption of a National Strategy regarding cyber security of network and information system (1a), creation of cooperation group to facilitate strategic cooperation/ exchange of data(1b), network for answering regarding digital incident (c), designation of national authority
EUR-LEX, Directive (EU) 2016/1148 of the European Parliament and of the Council of the 6/07/2016 concerning measures for a high common level of security of network and information system across the Union (document 32016L1148).
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148

III) Results and main challenges.

As we have just mentioned, the European projects set up in Georgia should be in line with Georgian needs. It is nonetheless interesting to see whether the results are in line with expectations (a). This will be the first parameter chosen to measure the effectiveness of the project. Secondly, beyond strengthening cyber security in Georgia, the objective is also to become closer to the partner of the EU, especially in view of Georgia's much-desired candidate status (b). Efficiency will therefore be measured by these two parameters. One is the primary objective (strengthening cyber security, through infrastructure, human capital requirements, etc.). The other is the implicit objective behind all these projects. Finally, it will also be a question of preserving future general challenges in Georgia (c).

a) A stronger cyber sector?

To see how Georgia is evolving and progressing, we need to look at the results of some of the projects discussed above. In this way, we can see whether Georgia's needs can be "met".

Georgia is one of the few countries to have defined a Critical Information System and has also set up a nationally-defined "information sharing mechanism" that crosses sectors. In line with its needs, public-private cooperation mechanisms have also been set up in the field of cyber security. Georgia has also defined penalties for cybercrimes.[82] If we look at the overall assessment of policy maturity, we can see that Georgia has 8 out of 10 areas of "managed"[83]. Two areas are still at the "initial" stage: essential service and cooperation mechanism). Regarding "essential service", this means that there is legislation, but that it is not relevant to CII operators, and there is not necessarily a distinction between CI and CII operators. For cooperation mechanism: there are policies related to the cooperation mechanism but there is no formal mechanism to share information. There is not really an entity specifically dedicated to reporting mechanisms, and public and private cooperation is at an immature stage[84]. Similarly, there is no cyber contingency plan at national level, only in certain sectors such as banking. Similarly, there are no unified budgets. Nevertheless, it is important to emphasize that Georgia is one of the most advanced countries in the partnership. Georgia continues to make progress in the field of cyber security, in line with European standards. Moreover, it should be pointed out that this report dates from 2020. In reality, the real changes were made in 2021: the new Information Act was introduced in 2021. This is all the more true as Georgia had already adopted laws such as the Georgian Law on International Cooperation in Criminal Matters, which was not taken into account[85]. Overall, the criticisms set out in this report let the professional perplex[86]. On the criticism of the lack of resources, the situation has improved, but Georgia does not have infinite resources or means. Similarly, with regard to the lack of staff dedicated to cyber security, the criticism seems rather weak: there are more and more tailor-

---

[82] EU4Digital, Cybersecurity guidelines for the Eastern Partnership countries, June 2020. 46p. https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf

[83] "Managed" is the second step in the implementations. Some things have been done for this, but there is still something to do. It is situated between "Initial" (almost nothing is done), and "defined" (very well advanced).

[84] EU4Digital, Cybersecurity guidelines for the Eastern Partnership countries, June 2020. 46p. https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf

[85] Legislative Herald of Georgia, Law of Georgia on International Cooperation in Criminal Matters, consolidated versions 2016-2018. https://matsne.gov.ge/en/document/view/112594?publication=4

[86] Interview with a cyber domain professional

made courses. The cyber security community does not rely on university education, which is insufficient to meet practical requirements. Nevertheless, the level of awareness in civil society remains low. However, comparing to previous time, cyber security has completely changed. Notably, Georgia has new players, new regulators (including government agencies, Cyber Security Bureau, SSCG,…). Regarding the cooperation between private and public sectors, we can say that it is still at the beginning stage, but the framework already exists. Georgia is doing this by itself. It is also essential to clarify that the cyber security reforms undertaken in Georgia go beyond the Agreement. Finally, the Agreement remains a solid basis for the development of new projects in Georgia[87].

Looking at the twinning project, we can firstly observe that Georgia is becoming aware of its shortcomings. On 3 April 2023 a conference was held on "Cyber Public Private partnership". Admittedly, this is a primary development state. However, it does mean that Georgia is setting up forums for discussion and the exchange of ideas, also with the aim of highlighting the importance of this partnership, while trying to find the most appropriate solution possible. Similarly, the NIS2 directive seems to intrigue Georgia: the country is to host a training project. Integrating the NIS2 directive implies major new changes, and the strengthening of the field of cyber security in Georgia. It has to be noted that NIS 2 is not yet mandatory for Member States. Georgia will probably join as soon as it is made mandatory. Moreover, NIS Directive has been useful, especially on capacity building and training, but overall in raising cyber capacities in Georgia[88]. Several changes have been made as a result of the NIS directive, particularly in terms of response procedures. Also, Georgia is continuing its assiduous work to ensure that it is fully in line with European expectations. In particular, special cooperation has been put in place between Lithuania, Austria and Georgia to facilitate the implementation of European requirements[89]. The institutional governance model has also been strengthened. Developing cybersecurity has required the creation of a structured definition and appropriate institutional functioning, which has led to a strengthening of the institutional model. The designation of guiding entities in the field, of competent governmental authorities, the structuring of a strategy (also in line with European requirements), the identification of stakeholders, etc., are all part of this process.

To conclude, in terms of advances in cyber security, Georgia has really improved its framework. Georgian legislation on cybercrime therefore complies with European principles and rules in both form and substance. In particular, the NIS Directive has been rather useful to the Georgian framework. Several changes were then introduced, including a change in the information security law, which broadened the definition of CNI (no longer just state entities, but also telecommunications providers and other private sectors). The NIS directive has had an impact on international cooperation, data exchange, etc. The agenda was ambitious, but the results have been good for Georgia. Moreover, the European framework can potentially provide a guideline for Georgia, which can then improve its own system, while benefiting from European support[90]. We could say that in terms of cyber security, it has been effective.

---

[87] Akhvlediani Tinatin, The new Eastern Partnership- what's in it for Georgia, 11/06/2020. https://gip.ge/the-new-eastern-partnership-whats-in-it-for-georgia/

[88] Interview with a cyber domain professional

[89] EU Twinning for Strengthening Cybersecurity in Georgia, Facebook. https://www.facebook.com/cybersecgeorgia/

[90] Akhvlediani Tinatin, Digital and cyber dimensions of the EU association agreements with Georgia, Moldova and Ukraine. 17p. 12/12/2019. https://3dcftas.eu/publications/digital-and-cyber-dimensions-of-the-eu-association-agreements-with-georgia-moldova-and-ukraine

However, it is still interesting to consider the effectiveness regarding the links with the European Union…

b) Closer ties with the European Union?

Looking at Georgia's international agenda, it's impossible to miss the will, at least of the population, to join the European Union. The desire to move closer together and apply for candidate status is a burning issue in Georgia right now. Indeed, the objective of cooperation such as cyber security seems undeniable. Of course, strengthening and solidifying a partner country makes sense, but it would be unwise to ignore the fact that this cooperation also implies the creation or reinforcement of new links. Georgia is the first EaP country to comply with European directives[91]. In this sense, measuring the effectiveness of this cooperation cannot only take cyber security into account, especially in view of the Georgian situation in 2023.

Regarding points 2 and 6 of the twelve priorities, we can look forward to strengthened and fruitful cooperation. In particular to the fight against organized crime, Georgia is rather active: arrest of skimmers, arrest of members of organized crime groups, etc. The idea is obviously not to reduce threats, which is impossible, but at least to put in place an effective response. For example, the latest major operation was the Goznym case, in which Georgia cooperated with EuroPol services, a sign of growing cooperation[92]. Fighting against organized crime, including cybercrime, was also part of the Association Agreement. The Spill Over Effect can be real, especially in view of the war unleashed by Russia in Ukraine. Georgia may be directly affected: spill over would therefore impact cyber security[93]. In fact, Georgia took part in a European mission in Mali, proving that the security sector as a whole is affected by cooperation between these two areas. The European Union takes Georgia's efforts into account.[94]

Thus, the cooperation in this specific sector has involved and can involve growing cooperation, particularly in the security sector in general. Of course, it would be precipitous to say that Georgia would achieve candidate status simply on the basis of its progress in the cyber security sector. Nevertheless, it's undeniable that Georgia is cooperating with the European Union, and that Spill Over isn't just a fanciful idea. Nevertheless, Georgia still faces other challenges…

c) Future and remaining challenges

Obviously, nothing is certain. Criticism is mounting over the current government, which is seen as ineffective in meeting European requirements, and specifically over the twelve priorities, for which the deadline is approaching. In this sense, links with the European Union and future cooperation are not guaranteed either. Similarly, even if cooperation with the European Union is a solid support, threats and challenges remain.

---

[91] Spinu Natalia, Georgia Cybersecurity, governance assessment, DCAF Geneva Centre for Security Sector Governance.15p. November 2020.
[92] EuroPol, Goznym Laware : cybercriminal network dismantled in international operation, 16/05/2019. https://www.europol.europa.eu/media-press/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation
[93] Interview with a cyber domain professional
[94] European Parliament, Association agreement between the EU and Georgia, European Implementation Assessment, (update), 66p. 2020. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/642820/EPRS_STU(2020)642820_EN.pdf

The main focus will be on business continuity. Indeed, this is also part of the ability to be prepared to face a threat, to have a solid system. Improvements in this area are therefore expected. So, almost as a matter of course, Georgia's key issues for the future are capacity building against cyber-attacks, and resilience. Georgia wants to be able to minimize downtime for critical services. The main threats continue to be Russian malicious activity[95].

Considering the above, and based on the words of professionals, we can say that the efficiency of this collaboration is palpable. The field of cyber security has been strengthened, as have links with the European Union. The challenges remain major, but the support of the European Union remains present, particularly in the field of security. Georgia also remains master of its own destiny. Progress in European-Georgian relations is also based on will, on choice. The Georgian government is at a turning point.

To conclude, European-Georgian cooperation in the field of cyber security is flourishing. The European Union has become increasingly sensitive to this issue. Its aim is, of course, to protect its territory, but also to become a leader in digital terms. This means securing its cyber space. Overall, the European Union has several ambitions, particularly on the international stage. Georgia, for its part, has understood for more than ten years the need to protect its maritime, land and cyber space. The threat of Russian attacks is palpable, all the more so in the current context. Therefore, in view of its needs, and in line with European requirements, Georgia benefits from this cooperation. Overall, we can say that both sides gain: the European Union secures a larger territory, and Georgia strengthens its cyber security, so essential to the functioning and survival of its own state. Thus, Georgia has seized the opportunity and complied with European standards. Several cooperation agreements have emerged, since 2014, and intensified. The agreements concluded over the years have been, in the eyes of professionals, fruitful and efficient, thanks to two main factors: the cyber security field has been strengthened, and links with the European Union have been strengthened. They also look forward to cooperation in other sectors. Nevertheless, and once again, not everything depends on past efforts. The current government also needs to fulfill the twelve priorities for further cooperation. Georgia still faces many challenges, although professionals already know what to focus on. However, cyber security in the form we have just described is not the only challenge. Indeed, the case of Caucasus Online is significant. The company is the only owner of an underwater fiber-optic cable. It provides Internet access to Georgia, Armenia, and Azerbaijan. The cable lies beneath the Black Sea. This area is highly sensitive to Russian attacks. Cyber security therefore also involves protecting one's own Internet network. If Russia gets its hands on these cables, it could well be using them for its own ends. Once again, this subject is not really discussed within the European-Georgian partnership. Nevertheless, Georgia needs to protect itself from any threats. We can therefore wonder whether, firstly, Georgia will consider discussing this subject with the European Union, and, secondly, whether specific means will be put in place.

[95] Interview with a cyber domain professional

Bibliography.

Article:

Akhvlediani Tinatin, Digital and cyber dimensions of the EU association agreements with Georgia, Moldova and Ukraine. 17p. 12/12/2019.
https://3dcftas.eu/publications/digital-and-cyber-dimensions-of-the-eu-association-agreements-with-georgia-moldova-and-ukraine

Akhvkediani Tinatin, The New Eastern Partnership- what's in it for Georgia? 11/06/2020.
https://gip.ge/the-new-eastern-partnership-whats-in-it-for-georgia/

Cybersecurity & infrastructure security agency, America's cyber defense agency, Russia Cyber Threat Overview and Advisories.
https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/russia#:~:text=The%20Russian%20government%20engages%20in,harm%20regional%20and%20international%20adversaries.

Cyber Risk GmbH, The NIS 2 Directive
https://www.nis-2-directive.com/

J.Smith David, Russian Cyber Strategy and the War Against Georgia, Atlantic Council, in Focus Quarterly, 17/01/2014.
https://www.atlanticcouncil.org/%20blogs/natosource/russian-cyber-policy-and-the-war-against-georgia/

Olivier Arthur, Cyber sécurité : que fait l'Union européenne, , in Toute l'Europe, 09.01.2023.
https://www.touteleurope.eu/economie-et-social/cybersecurite-que-fait-l-union-europeenne/

Przemyslaw Roguski, Russian Cyber Attacks against Georgia, Public attributions and sovereignty in Cyberspace, in Just Security. 06/03/2020.
https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/

Rabussier Camille, L'application du droit international dans le cyberespace, Université Paris II Panthéon Assas, 102p. 2019.
https://idc.u-paris2.fr/sites/default/files/memoires/Mémoire%20Camille%20Rabussier%20Application%20du%20droit%20international%20dans%20le%20cyberespace.pdf

Scheelen Yannick, Machilsen Koen, Deprez Andy, How to prepare for the NIS2 Directive? On EY. 16/05/2023.
https://www.ey.com/en_be/cybersecurity/how-to-prepare-for-the-nis2-directive

Tielidze Giorgi, Russia's changed attack tactics and vectors in cyberspace, Georgian foundation for strategic and international studies, Expert Opinion n°171, 14p. 2021. https://gfsis.org.ge/publications/view-opinion-paper/171

Book:

Haas B Ernst, Beyond the Nation-State: Functionalism and International Organization, Stanford University Press, 584p. 1964.

Legal document:

Council Decision, decision concerning restrictive measures against cyber-attacks threatening the Union or its Member States. 30/07/2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020D1127

EUR-LEX, Directive (EU) 2016/1148 of the European Parliament and of the Council of the 6/07/2016 concerning measures for a high common level of security of network and information system across the Union (document 32016L1148). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148
Legislative Herald of Georgia, Law of Georgia on International Cooperation in Criminal Matters, consolidated versions 2016-2018. https://matsne.gov.ge/en/document/view/112594?publication=4

Legislative Herald of Georgia, Law of Georgia on Information security, consolidated versions 2015-2020 https://matsne.gov.ge/en/document/view/1679424?publication=3

Legislative Herald of Georgia, On the Establishment of the Legal Entity Under Public Law (LEPL) Called the Data Exchange Agency, consolidated versions 2012-2017. https://matsne.gov.ge/en/document/view/89662?publication=1

Official Journal of the EU, Association Agreement between the EU and the EAEC and their Member States, of the one part, and Georgia, of the other part. 261/4- 261/743. 30/08/2014. https://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=CELEX:22014A0830(02)

Newspaper:

Agenda GE, Georgia ranks 55th in the world, 30th in Europe for cyber security, 1/07/2021. https://agenda.ge/en/news/2021/1800

Civil Georgia, Georgia adopts cybersecurity strategy for 2021-2024, 07/10/2021. https://civil.ge/archives/446772

Reuters, UK announces support to protect Georgia against Russian cyber attacks, 29/06/2022. https://www.reuters.com/technology/uk-announces-support-protect-georgia-against-russian-cyber-attacks-2022-06-29/

Official website :

ANSSI (Agence nationale de la sécurité des systèmes d'informations), adoption de la directive NIS : l'ANSSI, pilote de la transposition en France. 2016.
https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

Delegation of the European Union to Georgia, The European Union supports cyber security bureau through advanced technological capacities to enhance cybersecurity in Georgia, 30/06/2021.
https://www.eeas.europa.eu/delegations/georgia/european-union-supports-cyber-security-bureau-through-advanced-technological_en

EaP Connect.
https://eapconnect.eu/

EEAS Europa, The Twelve Priorities.
https://www.eeas.europa.eu/sites/default/files/documents/12%20Priorities.pdf

EU4Digital, Cybersecurity guidelines for the Eastern Partner countries, 37p. June 2020.
https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf

EU4Digital, Georgia
https://eufordigital.eu/countries/georgia/

EU4Digital, Strengthening cyber-security expertise in Georgia, 30/07/2019
https://eufordigital.eu/strengthening-cyber-security-expertise-in-georgia/

ENISA, European Union Agency for Cybersecurity. Established in 2004, ENISA has been strengthened by the EU Cybersecurity Act.
https://www.enisa.europa.eu/about-enisa

European Commission, Cybersecurity policies
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

European Commission, Strengthening Cybersecurity capacities in Georgia, 48p.
https://um.fi/documents/385176/0/Strengthening+Cybersecurity+Capacities+in+Georgia.pdf/58a7bd7d-e7bd-af0b-8f61-d7da4428f2c9?t=1582806899150

European Commission, The EU Cyber Solidarity Act.
https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

European Commission, The Cybersecurity Strategy
https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

European Council, Council of the EU, Cybersecurity: how the EU tackles cyber threats, last reviewed on 24 May 2023.
https://www.consilium.europa.eu/en/policies/cybersecurity/

European Council, Council of the EU, Strengthening EU-wide cybersecurity and resilience-provisional agreement by the Council and the European Parliament.

https://www.consilium.europa.eu/en/press/press-releases/2022/05/13/renforcer-la-cybersecurite-et-la-resilience-a-l-echelle-de-l-ue-accord-provisoire-du-conseil-et-du-parlement-europeen/

European Union External Action, EU imposes first ever cyber sanctions to protect itself from cyber-attacks. 30/07/2020.
https://www.eeas.europa.eu/eeas/eu-imposes-first-ever-cyber-sanctions-protect-itself-cyber-attacks_en

Georgian Research and Educational Networking Association.
https://www.grena.ge/eng

The European Union for Georgia, Strengthening Cybersecurity capacities in Georgia.
https://eu4georgia.eu/projects/eu-project-page/?id=1458

Think Tank:

Think Tank Russia's war on Ukraine: Timeline of cyber-attacks. 21/06/2022.
https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549

Specialized documents.

Conseil de l'Europe, Convention on Cybercrime, European Treaty Series, n°185, 22p. 2001
https://rm.coe.int/1680081561

Consilium Europa, Facts and Figures about EU-Georgia Relations, 3p.
https://www.consilium.europa.eu/media/44400/685-annex-5-d-georgia-factsheet.pdf

Consilium Europa, Joint Declaration of the Eastern Partnership (Riga, 21-22 May 2015). 13p.
https://www.consilium.europa.eu/media/21526/riga-declaration-220515-final.pdf

CyberEast, Fact Sheet, 1p. March 2022.
https://rm.coe.int/cybereast-factsheet-march22/1680a5cc24

Cyber Security Bureau, Cyber Security Strategy of the Ministry of Defence of Georgia 2021-2024, 15p.
https://mod.gov.ge/uploads/Cyber_Security/Cyber_Security_Strategy_of_the_Ministry_of_Defence_of_Georgia_2021-2024%E2%80%9C.pdf

Cyber Security Strategy of Georgia, 2012-2015. 12p.
https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Georgia_2012_National%20Cyber%20Security%20Strategy%20of%20Georgia_ENG.pdf

EU4Digital, Cybersecurity guideline for the EaP, 46p. June 2020
https://eufordigital.eu/wp-content/uploads/2020/10/Cybersecurity-guidelines-for-the-Eastern-Partner-countries.pdf

European Parliament, Association agreement between the EU and Georgia- European Implementation Assessment (update), 67p. April 2020.

https://www.europarl.europa.eu/RegData/etudes/STUD/2020/642820/EPRS_STU(2020)642820_EN.pdf

EuroPol, Goznym Laware: cybercriminal network dismantled in international operation, 16/05/2019.
https://www.europol.europa.eu/media-press/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

GeoStat, National Statistics Office of Georgia, Indicators of using information and communication technologies in the households, 2021. 11p.
https://www.geostat.ge/media/40378/Indicators-of-Using-ICT-in-Households---2021.pdf

International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Tallinn Manuel on the International law applicable to cyber warfare, Cambridge University Press. 282p. 2013.
https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

Ministère des Armées, Droit International appliqué aux opérations dans le cyberespace. 18p.
https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqué%20aux%20opérations%20dans%20le%20cyberespace.pdf

Ministry of Defense (Georgia), Threat Assessment for 2010-2013.
https://mod.gov.ge/uploads/2018/pdf/TAD-ENG.pdf

Spinu Natalia, Georgia Cybersecurity, governance assessment, Geneva Centre for security Sector Governance, 14p. November 2020.
https://www.dcaf.ch/sites/default/files/publications/documents/GeorgiaCybersecurityGovernanceAssessment.pdf

World Economic Forum, Global Cybersecurity outlook 2023, Insight report, 36p. January 2023.
https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

Website:

Facebook, EU Twinning for Strengthening Cybersecurity in Georgia.
https://www.facebook.com/cybersecgeorgia/

Glossary.

Budapest Convention: Convention on Cybercrime (2001), bringing together 67 signatory countries. It provides for the criminalization of a list of attacks against and by means of computers, procedural law tools to make cybercrime investigations more effective, and the securing of electronic evidence. Emphasis is also placed on guaranteeing the rule of law. It takes into account and seeks to promote international police and judicial cooperation in cybercrime and electronic evidence. The Georgian legal framework on cybercrime covers all offences, as required by the Convention. The Convention therefore provides a secure and

effective framework. It also proposes actions to be taken at regional and national level. This framework makes it possible to share experience and facilitate cooperation.

CFSP: the Common Foreign and Security Policy aims to preserve peace and strengthen international security in accordance with the principles of the UN Charter. To enable the European Union to play a political role on the international stage, the Maastricht Treaty established a common foreign and security policy, which could eventually lead to a common defense policy. About Georgia, the European Parliament would like to strengthen cooperation on security issues, particularly cyber security and hybrid threats. It would also like to invite Georgia to take part in the PESCO project and strengthen its diplomatic presence.
Civil Service Bureau (CSB): Legal entity of public law, responsible for promoting the implementation of centralized policy. The CSB cooperates with International Organizations (PDP, GGI-USAID, UNDP).

Cyber-resilience: The ability of an information system to withstand cyber-attacks and return to a satisfactory state of operation and security. It includes the technologies and control processes designed to protect individuals and organizations against cybercrime. The NIS Directive requires organizations operating in critical sectors to achieve a high level of cyber resilience.

Digital Single Market: A policy pursued by the Commission since 2015, and one of its political priorities, it is made up of three pillars.
1) Improving access to digital goods and services, for example by removing obstacles to cross-border e-commerce while guaranteeing consumer protection.
2) An environment in which digital networks and services can flourish (high-speed, secure, and trustworthy infrastructures supported by regulatory provisions. The emphasis is on data protection, online privacy, fairness, and transparency).
3) Digital as an engine for growth.

In concrete terms, a number of measures have already been taken banning unjustified geographical blockades (2018), abolition of roaming charges (2017), revision of the regulation on cooperation in the field of consumer protection, and so on.
The intention is also to regulate the digital space, which has been done through two European regulations: the law on digital services (2022), and the law on the digital market (2022).
The European Union hopes to extend the benefits obtained to partner countries such as Armenia, Azerbaijan, Georgia, Ukraine and the Republic of Moldova.

EaP Connect: provides infrastructure and digital solutions for the research community in the six countries participating in the Eastern Partnership. It tasks are establishing and operate a high-capacity network for research & education, integrating national research and education network with the pan-European GÉANT network, this bridging the digital gap, deploying services that facilitate international cooperation and stimulate integration with GÉANT and other European e-infrastructure,…

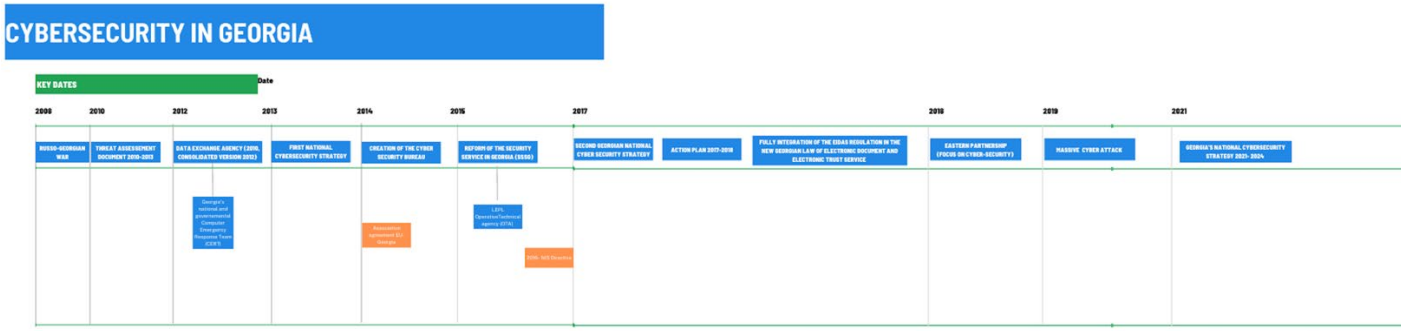
Eastern Partnership: Launched in 2009, the partnership includes EU member states and six partner countries: Armenia, Azerbaijan, Belarus, Georgia, the Republic of Moldova and Ukraine. The aim is to strengthen and deepen political and economic relations between the EU, its Member States and the partner countries, while supporting sustainable reforms in these countries. The partnership combines multilateral and bilateral components. The overall

objective is to increase the stability, prosperity and resilience of the neighbors, and is fully aligned with the European Commission's Strategic Program 2019-2024.
The partnership covers several areas: transport, energy, trade, civil society and digital technology.

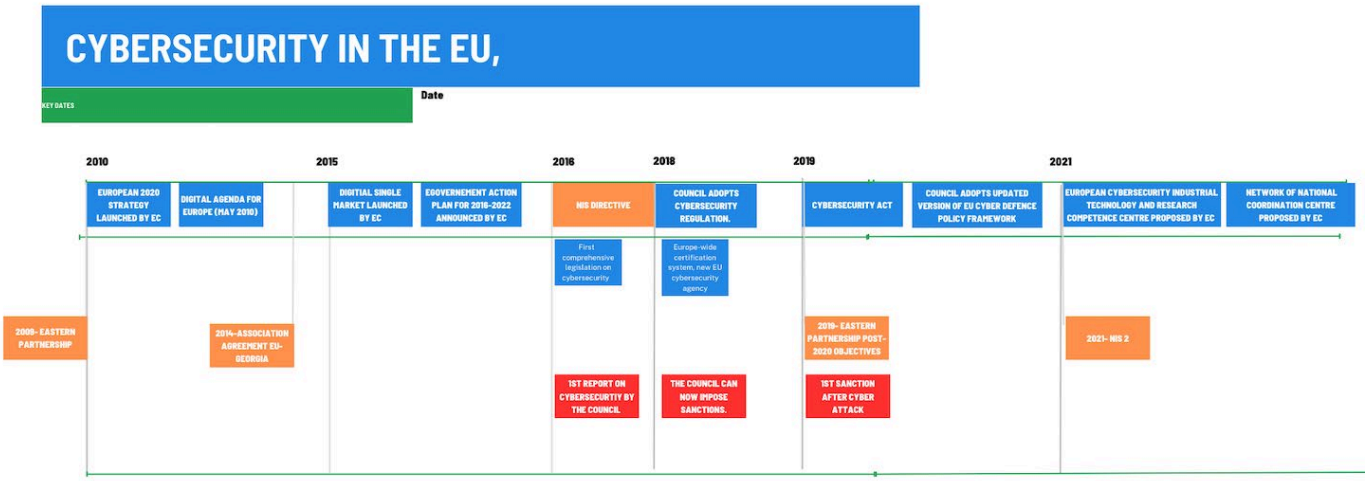
eIDAS: electronic identification, authentification and trust services. It establishes the framework to ensure that electronic interactions between businesses are safer, faster, more efficient. Basically, this European regulation created a single framework for electronic identifications and trust services.

Spill Over: Developed by Haas in 1964, this is the idea that state integration of an area A (or economic sector) will probably imply integration of area B, since strong links will be created. For example, trade integration is likely to imply integration in the customs sector to encourage the intensification of trade.

Annexes.



Annex n°1- Cyber-security in Georgia



Annex n°2. Cyber- security in the EU