Strengthening the national cybersecurity of Georgia

EaP Security Forum

Irakli Jgharkava

The policy brief is part of the **project „Eastern Partnership Security Forum**", that aims to launch the "EaP Security Forum" that will engage nongovernmental and governmental experts from Georgia, Moldova, Ukraine in a joint effort to strengthen security resilience of their countries in the areas of cybersecurity, intelligence reform, offsetting hybrid threats, and strengthening the national defense.

The project is funded by the Konrad Adenauer Stiftung (KAS) and implemented by the Foreign Policy Association of Moldova in partnership with the Georgian Center for Strategy and Development and the Foreign Policy Council "Ukrainian Prism".

Disclaimer: The information and opinions provided in this analytical material belong to the author and do not necessarily reflect the views of the donor.

SUMMARY

This paper examines Georgia's cybersecurity policy, current threats to the country, and the challenges and opportunities offered by the "Association Trio" platform recently initiated by Georgia, Ukraine, and Moldova. Georgia has made solid progress in reshaping its cybersecurity strategy, but recent figures (2020 GCI report) indicate that its cyber capabilities seem to have deteriorated, and suggest the need for a new cyber vision to meet the current challenges.

Although the steps taken by the state in recent years to create more structural support for cyber security policy are unequivocally positive, the implementation of this policy is problematic. According to the subject-matter experts, this is due to the fact that the cyberspace-related threats are not taken seriously at the governmental level, and government agencies and employees lack 'cyber awareness'.

The Association Trio countries want to enhance their security and defense capabilities by cooperating to counter hybrid threats, strengthening their cyber resilience, developing cooperation platforms with the EU Hybrid Fusion Cell and EU Cyber Security Agency, participating in CSDP (The Common Security and Defense Policy) missions and operations, and participating in the EU Permanent Structured Cooperation (PESCO) projects.

INTRODUCTION

Georgia's cyberspace has been the target of attacks since the war with Russia that took place in August of 2008,[1] and it is one of the most vulnerable areas of the country's security architecture. The Association Trio[2] platform is an opportunity to strengthen the cybersecurity space -through strategic partnerships. The participating states of the Associated Trio are members of the European Union 's Eastern Partnership region, which is united by the goal of achieving integration with the EU institutions. Georgia now has a chance to cooperate with the EU on cybersecurity, which is one of the highlighted objectives of the agreement.

This paper will study the current risks, challenges, and opportunities for Georgia's cybersecurity policy, as well as examine the possibilities and opportunities for the Association Trio countries to cooperate with the EU and strengthen their cybersecurity.

POLICY EVALUATION

Threats and Challenges for Georgia's Cyberspace

Although Georgia was one of the first countries to acknowledge the need for a solid cybersecurity policy, the cyberspace-related challenges have also grown significantly. The orchestrated cyberattack on the databases of the Richard Lugar Public Health Research Center in September 2020[3] proved that Georgia is still far from having an effective cyber defense policy.

The growing concern over cybersecurity-related vulnerability stems from the rapid development of information technologies, which led to the dependence on modern electronic systems. Public services, public infrastructure, and security systems depend on constant updates of digital technologies, and this naturally generates both external and domestic risks. The lack of public awareness of cybersecurity threats and cyber espionage exacerbates the cyberspace challenges. One of the cybercriminals' main targets is the financial and banking sector. A successful cyberattack on Georgia's banking system could financially devastate its citizens.[4]

Russia has attacked Georgia's critical infrastructure since 2008, and is now the area that causes the most concern for the Georgian security experts. Just before the 2008 Russian invasion of Georgia, Russian cyberattacks targeted government agencies, the media, and the banking sector, severely damaging the country's critical infrastructure. This was the very first time when a cyberattack had been carried out in conjunction with an armed conflict.[5] Since then, Georgia has repeatedly been the target of cyberattacks from Russia, including the

[1] Davit J. Smith, "*Russian Cyber Strategy and the War Against Georgia,"* Atlantic Council, Available at the following link (consulted on: 25.08.2021).
[2] Rahim Rahimov, "*Georgia, Ukraine, Moldova Form an Association Trio,"* Eurasia Daily Monitor, Volume: 18 Issue: 91, Available at the following link (consulted on: 25.08.2021).
[3] "*Cyberattack on the Ministry of Health and Russian Trace*," Institute for Development of Freedom of Information (IDFI), Available at the following link (consulted on: 29.08.2021).
[4] Irakli Jgharkava, "*Georgia's Cybersecurity Policy, Challenges, and Opportunities,*" Georgian Center for Security and Development (GCSD), Available at the following link (consulted on: 27.08.2021).
[5] *Ibid*

large-scale attack from October 2019[6] and the cyberattack on the Richard Lugar Public Health Research Center from September of 2020. For Russia, cyber-attacks are important components of the psychological manipulation and information warfare. They weaken Russia's adversaries by creating public distrust in the adversary's government, and harm the national security of the target country. The Kremlin has aggressively increased the state's cyber-attack potential and expanded the scope of Russia's cyber-operations. Andro Gotsiridze, a cybersecurity expert,[7] has noted that, like everyone else, Georgia's dependence on information and communication technologies has increased significantly since 2008, which increases the amount and extent of the damage that a cyber-attack could inflict.

Fighting cyber espionage is especially important. As a result of cyber espionage, cyber-criminals may have access to information about state secrets, which could greatly harm Georgia's national security. Cyber espionage techniques include phishing and infecting the computer systems of the public agencies. According to Gotsiridze, the low level of 'cyber awareness' among Georgia's government employees makes cyber espionage easier because they are not able to pick up clues that an attack is occurring until after it already happens and do not know how to set up or maintain their agency's computerized systems to block such attacks.[6]
Information Warfare is a serious challenge for Georgia. The propaganda and fake news that spread through cyber channels may have a bad psychological effect: changing the public opinion to favor the Kremlin, reducing pro-Western sentiments, and forming and strengthening the pro-Russian elite (agents of Russian influence) in Georgia.[8]

Georgia's major achievements in cybersecurity policy

As a result of Russia's combined ground, air, naval cyber-attacks on Georgia in 2008, Georgia was one of the first countries to develop a state policy in the field of cybersecurity. These cyber-attacks have signaled that the protection of the cyberspace is as important for ensuring national security as is the protection of the land, air, and sea. The Law on Information Security, put into effect in 2012, regulates the state cybersecurity and represented a step forward in this regard. Georgia's Cybersecurity Strategy and Action Plan was developed in 2013-2015 and later updated in 2017-2018. Several cybersecurity structures have been established within the Ministry of Defense (the Cybersecurity Bureau), the Ministry of Internal Affairs (the Cybercrime Bureau), and the Ministry of Justice (the Digital Governance Agency). A minimum standard of information security has been established, and the concept of "critical information system subject" has been introduced.[9]

According to the cybersecurity expert Vladimer Svanadze, 2017 was the most successful year for Georgia in the field of/in terms of cybersecurity, when it ranked eighth in the world, eighth in the European region, and first among the Commonwealth of Independent States (CIS) countries according to the International Telecommunication Union (ITU) and the Global Cybersecurity Index (GCI). In a study published by the e-Governance Academy (eGA) in the same year, Georgia ranked second in the European region, which was a great achievement for the country.[10] In addition, the Parliament of Georgia passed amendments to the Law on Information Security on June 10, 2021. The amendments introduced three separate categories of "critical information system subjects" and established administrative sanctions for violating information security-related requirements. These amendments will come into force on December 30, 2021.

---

[6] "*Georgia hit by massive cyber-attack*," BBC, Available at the following link (consulted on: 30.08.2021)
[7] Andro Gotsiridze, Cybersecurity consultant, Cyber Security Studies & Education Center (CySec), Interview, August, 23, 2021.
[8] *Ibid*
[9] Irakli Jgharkava, "*Georgia's Cybersecurity Policy, Challenges, and Opportunities*," Georgian Center for Security and Development (GCSD), Available at the following link (consulted on: 27.08.2021).
[10] Vladmier Svanadze, Director of Georgian Academy of Technological Innovations, Interview, August 23, 20221.

The amendments also define the powers of the Operative-Technical Agency, the creation of which has created concerns about ambiguity in security matters. The Operative-Technical Agency is under the auspices of the State Security Service, Georgia's chief domestic intelligence authority. The Institute for the Development of Freedom Information (IDFI), a local watchdog, considers this a problem because it means that the Operative-Technical Agency has direct access to information systems in the telecommunications sector and the legislative, executive, and judicial branches of the government, and also has indirect access to personal and commercial information stored in these systems.[11] Yet, another ambiguity is the absence of the Single Point of Contact (SPoC) on cybersecurity matters, which is a serious problem;[12] but there is, nonetheless, a strong foundation on which Georgia can build its future cybersecurity.

By 2020, according to the 2020 GCI report, Georgia's cyber capabilities had deteriorated. The country ranked 55th in the world in cybersecurity, with 81.06 points, and was the 30th in the European region rankings, with 81.07 points.[13] Although the steps taken by the state in recent years to create more structural support for cyber security policy are unequivocally positive, the implementation of this policy is problematic. According to the subject-matter experts, this is due to the fact that the cyberspace-related threats are not taken seriously at the governmental level, and government agencies and employees lack 'cyber awareness'. In addition, policies change, whether they are beneficial or harmful, every time a new administration comes into power. New government administrations in Georgia want to create their own infrastructures and usually dispose to get rid of the old ones. This is an unhealthy attitude and practice that wastes time and resources, and threatens a variety of matters that are critical to the national security of the country.

ASSOCIATED TRIO: A CHANCE FOR GEORGIA TO STRENGTHEN ITS CYBER RESILIENCE

The foreign ministers of Georgia, Ukraine, and Moldova formed the Association Trio on May 17, 2021, in Kyiv and signed a Memorandum of Understanding that established their cooperation on European integration.[14] The main goal of the newly formed alliance is to collectively find ways to speed up the membership in the European Union (EU). Other goals address the cooperation with the EU on transport, energy, digital transformation, green economy, justice and home affairs, strategic communications, and healthcare-related matters.

The Association Trio countries want to enhance their security and defense capabilities by cooperating to counter hybrid threats, strengthening their cyber resilience, developing cooperation platforms with the EU Hybrid Fusion Cell and EU Cyber Security Agency, participating in CSDP (The Common Security and Defense Policy) missions and operations, and participating in the EU Permanent Structured Cooperation (PESCO) projects.[15] It is worth noting that the hybrid threats stemming from Russia that aim to disrupt their EU ambitions represent one of the main factors that link together the Association Trio countries. As such, the new cooperation platform is an opportunity for the participating states to strengthen their cyber resilience, as well as find a joint solution to counter the challenges they face.

The Association Trio also has the potential to deepen the strategic partnerships among the three countries on cybersecurity matters. One example of a useful initiative could be the development and establishment of a **joint platform for information sharing on cyber-related incidents, cyber threats, and vulnerabilities.** This could

[11] "*Parliament Passes Controversial Information Security Laws*," Civil.ge, Available at the following link (consulted on: 31.08.2021).
[12] Giorgi Iashvili, Georgian Information Security Association, Interview, August 30, 2021.
[13] Vladmier Svanadze, Director of Georgian Academy of Technological Innovations, Interview, August 23, 20221.
14 Vlagyiszlav Makszimov, "*Georgia, Moldova, Ukraine formalise their higher EU ambition,*" EURACTIV, Available at the following link (consulted on: 30.08.2021).
15 „*Association Trio: Memorandum of Understanding between the Ministry of Foreign Affairs of Ukraine, Ministry of Foreign Affairs of Georgia and the Ministry of Foreign Affairs and European Integration of the Republic of Moldova,"* Ministry of Foreign Affairs of Ukraine, Available at the following link (consulted on: 28.08.2021).

boost the countries' cyber capabilities and increase their readiness to counter future possible attacks on critical infrastructure. The joint platform could involve and bring together think-tanks, the academia, and the energy sector, and include mutual technical assistance, and joint exercises and trainings to enhance the nations' cyber capability. According to the GCI 2020 Report, Georgia, Ukraine, and Moldova have different GCI rankings in Europe (30th, 39th, and 33rd, respectively), this is why cooperation and the exchange of ideas and assistance could substantially benefit all of them.

The Association Trio must consider developing a smart defense against common security challenges, especially in cyberspace, by sharing their strengths, setting joint goals and priorities, and coordinating their defensive efforts. When their strategic partnership is established, the Association Trio must work on extending the cyberspace policy cooperation opportunities to include the European Union. Sharing information on cyber incidents could benefit both sides. In this regard, gaining access to and cooperating with the European Union Agency for Cybersecurity (ENISA) will be a strategic breakthrough for the Association Trio, which could speed up their integration into the EU.

CONCLUSIONS AND RECOMMENDATIONS

Although, Georgia has been one of the pioneers in developing state cybersecurity policy, the implementation of the policy, its new rules and procedures remains to be a challenge. As technology evolves, so will the risks and threats to cyberspace. Identifying such risks before they occur and creating appropriate countermeasures will be critical. Hopefully, the newly created Association Trio alliance will help each country achieve these goals and strengthen their individual defenses. Considering Russia's persistent cyber-attacks against the Association Trio countries, not doing so may hinder their integration into the European Union because other countries in the EU will not welcome partners that cannot effectively defend themselves and that pose a security risk to all.

Recommendations for Georgia:

- It is crucial to develop a new cybersecurity strategy that can reflect the current challenges in the cyberspace in the short, medium, and long terms.
- Because getting government agencies in Georgia to adopt consistent policies is difficult, especially in the field of cybersecurity, which many do not consider to represent a real threat, Georgia should create an independent executive office or agency that could handle the cybersecurity issues and keep track of and weigh the importance of cybersecurity threats for every agency. It should also have the authority to impose effective cybersecurity defensive measures in all areas of government activity in a coordinated and centrally administered fashion.
- Georgia should adopt the security measures set by the International Organization for Standardization (ISO), the U.S. National Institute of Standards and Technology (NIST), and the Information Systems Audit and Control Association (ISACA). These measures should be used by all public service providers, including private government contractors, to ensure Georgia's national security.
- Georgia should develop Public-Private Partnerships (PPPs) in cybersecurity. Georgia does not have enough cybersecurity professionals to counter current cybersecurity threats, therefore, it is necessary to use and involve outside providers and professionals from the private sector.
- Georgia should not only develop a comprehensive cyber defense policy and cyber defense capabilities but should also work on good cyber offenses, to counter the hybrid threats it is exposed to and send a message to those who want to attack Georgia's critical infrastructure.

Recommendations for the Association Trio:

- Develop a strategic partnership in the field of cybersecurity by setting up a common platform that records information on cyber-related incidents, threats, and vulnerabilities. Knowledge and experience should also be exchanged among the three countries, joint exercises and trainings should be conducted, the countries should cooperate on technical matters, and they should all work on developing public-private cybersecurity partnerships.
- Develop a strategic partnership and cooperate with the European Union on cybersecurity. Getting access to the ENISA platform would not only benefit the Trio, it would also be a step towards the integration with the EU.

ABBREVIATIONS:

CSDP - Common Security and Defense Policy
EaP - Eastern Partnership
eGA - e-Governance Academy
ENISA - European Union Agency for Cybersecurity
GCI - Global Cybersecurity Index
ISACA - Information Systems Audit and Control Association
ISO - International Organization for Standardization
ITU - International Telecommunication Union
NIST- National Institute of Standards and Technology
PESCO - Permanent Structured Cooperation

ABOUT THE AUTHOR

Irakli Jgharkava is International Relations and Security specialist. He holds three master's degrees from the following disciplines: Managing Disruption and Violence (Daniel Morgan Graduate School of National Security, Washington, DC, USA), where he studied Russia's strategy towards NATO and Georgia; European Interdisciplinary Studies (College of Europe) with the focus on the impact of the EU "Transformative Power" on Georgia's Europeanization (Association Agreement, DCFTA); Nationalism and Ethnicity Studies (Tbilisi State University), focus on the impact of the 2015 migration crisis on the surge of ultranationalism in Europe. Irakli also holds a Bachelor's degree in International Relations from Tbilisi State University. His research interests include: national security, cyber security, information warfare, Georgia-EU relations.

ABOUT THE IMPLEMENTING ORGANIZATION

Foreign Policy Association of Moldova (APE) is one of the leading foreign policy think-tanks in Moldova. The Association is committed to supporting the integration ofthe Republic of Moldova into the European Union and facilitating the resolution of the Transnistrian conflict in the context of the country's Europeanization. APE was established in 2003 by a prominent group of local experts, public figures, former government officials and high-ranking diplomats, who decided to contribute throughtheir experience and expertise to the development of a coherent, credible and efficient foreign policy of the Republic of Moldova.

office@ape.md | www.ape.md | @APEMOLDOVA | @ape.md

ABOUT THE PARTNERS ORGANIZATIONS

Georgian Center for Strategy and Development (GCSD) is a non-partisan, non-governmental organization. Since its establishment, GCSD has directed efforts towards supporting Georgia's and regional sustainable, democratic development by embedding values of respect, impartiality, accountability, fairness and transparency in all interventions and undertakings. Over years GCSD has distinguished itself as an outstanding local think-tank. the organization has carried out number of research activities and issued remarkable publications, covering variety of topics. GCSD is the first Georgian organisation to establish a unit within its structure fully dedicated to research of topics related to terrorism, violent extremism and radicalisation. The Terrorism Research Center (TRC) of GCSD aims to increase the knowledge and awareness of the Georgian society regarding the above stated phenomena and to design and implement projects that help minimise the threat thereof.

gcsd@gcsd.org.ge | www.gcsd.org.ge | @GCSDorg | @GCSDorg

Foreign Policy Council "Ukrainian Prism" is a network-based non-governmental analytical center, the goal of which is to participate in providing democratic ground for developing and implementation of foreign and security policies by government authorities of Ukraine, implementation of international and nation-wide projects and programs, directed at improvement of foreign policy analysis and expertise, enhancement of expert community participation in a decision-making process in the spheres of foreign policy, international relations, public diplomacy. The Foreign Policy Council "Ukrainian Prism" is offcially registered as a non-governmental organization in 2015, while analytical work and research had been carried out within the network of foreign policy experts "Ukrainian Prism" since 2012. At present, the organization united more than 15 experts in the sphere of foreign policy, international relations, international security from different analytical and academic institutions in Kyiv, Odesa, Kharkiv, Chernihiv and Chernivtsi.

info@prismua.org | www.prismua.org | @prismUA | @PrismUA