Strengthening the national cybersecurity in Associated Trio: Georgia, Moldova & Ukraine

EaP Security Forum

CONTENT

The analytical synthesis are 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".

Foreign Policy Association APE Asociația pentru Politica Externă GCSD UKRAINIAN PRISM KONRAD ADENAUER STIFTUNG

STRENGTHENING THE NATIONAL CYBERSECURITY OF THE REPUBLIC OF MOLDOVA

by Natalia Stercul
Foreign Policy Association of Moldova

SUMMARY

The strengthening of the cybersecurity of the Republic of Moldova is gradually becoming an important area of the national security policy-making. Over the last decade, Moldova has made great efforts to develop the core of the national cybersecurity system. Despite this, the country remains extremely vulnerable to cyber threats, cyberattacks and cybercrime. The building of the national cybersecurity system was complicated by the lack of a holistic vision of a cybersecurity strategy, limited resources and technical possibilities to use mixed integrated security methods for the functioning of the system. The incidents that have occurred in recent years clearly illustrate the low level of Moldova's infrastructure preparedness to withstand massive cyberattacks against official state bodies, financial banking structures, public and private sectors.

After the signing of the EU-Moldova Association Agreement, a new phase in Moldova's national security development has begun. This period is marked by the deepening of the reforms initiated in previous years and the development of new policy documents, which attempted to address the gaps and failures identified in the previous stages. The EU initiatives and projects became an essential part of the ongoing cybersecurity developments in Georgia, Ukraine and Moldova.

In line with the new EU Cybersecurity Strategy and the establishment of a "European Cyber Shield" in EU countries, it is important to improve the operational capacity of the "Association Trio" group to increase the degree of information exchange between stakeholders and to provide timely warnings of potential cybersecurity incidents. The "Association Trio" platform demands a more active involvement of the EU in the security sector reforms, and a focus on both "soft" and "hard" power, using the large spectrum of instruments offered by the European Defence Fund (EDF) and the Permanent Structures Cooperation (PESCO) frameworks.

INTRODUCTION

The new round of the modern digital world development has increased the relevance of cybersecurity as one of the instruments for achieving the state's national interests. The existence of numerous cyber security issues in various spheres of life naturally increase the political interest in resolving those issues. The need for ensuring cybersecurity is growing, whether to address particular cases or those at the national and international levels, becoming a strategic challenge within diplomacy, domestic and foreign politics.

Moldova is in a continuous process of strengthening its cybersecurity at the national level, both in legal, institutional and technical terms, and efforts are being made in this regard by authorities that are responsible for providing security. Despite this, Moldova is faced with having to deal with challenges in all spheres – from cybersecurity capacity-building and developing policies to the ability to fully benefit from and explore all elements of the cyberspace. A strong digital expansion must be backed by robust cybersecurity measures. This is not easy to achieve, especially in Moldova's case. According to the National Cyber Security Index 2021, which includes cybersecurity data on 160 countries, Moldova ranks 58th and showcases low performances on nearly all general and baseline cybersecurity indicators.

THE CURRENT LANDSCAPE OF MOLDOVAN CYBERSECURITY SPACE: MAIN RISKS, THREATS AND CHALLENGES

Nowadays and more than ever before, Moldova faces a wide range of cyber threats, including against public institutions and private sector organizations, as well as ordinary citizens. A significant number of cybercrimes are being committed in Moldova, among them being the politicized hacker attacks, as well as various financial and non-financial crimes. In recent years, the government communication systems have become the target of coordinated mass attacks during periods of major political events. In particular, election campaigns in Moldova frequently led to the intensification of cyberattacks on state bodies handling the electoral process. According to the Analytical Review of ICT Regulatory Policy in Moldova, there were unprecedented attacks against the websites of state bodies, the Central Election Commission, observer organizations and the media.

From the data collected between 2014 and 2021, different vectors of attack in the cyber security space were identified. There is a tendency of malware infestation of business and corporate e-mails, which aim to compromise the security systems by exploiting the human factor. In June 2015, the National Bank of Moldova was targeted in a well-coordinated DDoS attack against its website, which led to its temporary shutdown. In the same year, the country's law enforcement agencies registered 13,000 cases of theft of funds from bank accounts. During 2018, within the cyberspace of the public authorities and private companies of the Republic of Moldova there were registered 127 418 cases of information systems and telecommunications networks that were infected with various types of malwares, which form a malicious botnet information infrastructure. According to a study from 2019 by ENISA, 94% of all malware types were delivered via e-mail. The top strains of malware targeting businesses were: Trojan.Emotet, Adware, InstallCore, HackTool. WinActivator, Riskware, BitCoinMiner and Virus, Renamer.

In 2020, a new wave of cybercrime has started with the beginning of the Covid-19 pandemic. Cyberattacks have become more frequent, especially ones that targeted critical infrastructures in the financial-banking, private and public sector. In July 2021, the Court of Auditors' public databases were destroyed following a cyberattack. Cyberattacks are now the fastest growing crime at the national, regional and global scale. The need to update Moldova's critical infrastructure and maintain a high level of cybersecurity against the threats of modern cyberattacks has become increasingly evident. Moldova, within its capabilities, has put effort into strengthening its cybersecurity capacity at both policy and technical levels. However, the increased frequency of cyber-attacks, as well as their level of sophistication are deeply disturbing and impacting the economy, finances, governance and the daily lives of the citizens.

MAIN REFORMS, POLICY ACHIEVEMENTS AND FAILURES IN STRENGTHENING THE NATIONAL CYBERSECURITY

Moldova has begun to take practical measures to address its cybersecurity issues after 2009, when the protests and riots that took place following the April 2009 elections were called by many a “Twitter revolution”. Since 2010, Moldova has focused more attention on the creation of institutional structures for cybersecurity at the national level. To contribute to the intensification of this process, in line with the Budapest Convention, the authorities created several institutions, centers and divisions, such as the National Center for Personal Data Protection of the Republic of Moldova (NCPDP), the General Prosecutor’s Office the Centre for Combating Cybercrime; the Security and Intelligence Service (SIS), the Cyber Security Center – CERT-GOV-MD. These created a certain basis for the institutional hierarchy that could ensure cybersecurity in Moldova and counteract attacks on the state’s information resources. With that being said, a more complex and effective approach to ensuring national cyberspace security is still needed.

In 2011 the Law № 133 on Personal Data Protection was adopted. One of the aims of the law was to ensure compliance with the EU Data Protection Directive 95/46. The Moldovan legislative body opted for a full application of personal data protection law in the criminal law area. A considerable step towards the creation of favorable conditions for and large-scale use of the ICT tools by public institutions, businesses and citizens, was the adoption of the decision № 857 of 31 October 2013 the "National Strategy for Information Society Development - Digital Moldova 2020". The creation of the current regulatory framework for the integrated support of cybersecurity in the Republic of Moldova represented one of the accomplishments achieved between 2014-2020. The period under review is marked by the deepening of the reforms initiated in previous years and the development of new policy documents. This stage starts with a political event - the signing of the EU-Moldova Association Agreement.

The basic document that regulates the creation and implementation of a cybersecurity management system is the National Cyber Security Program of the Republic of Moldova for 2016-2020, approved by the Government Decision № 811 of 29.10.2015. The document was elaborated in accordance with the provisions of the Moldova-EU Association Agreement, the Council of Europe Convention on Cybercrime, the EU Cyber Security Strategy, the Recommendations of the International Telecommunication Union on cybersecurity for electronic communications networks and the National Security Strategy of the Republic of Moldova.

The need for an integrated system for reporting and assessing information security threats and developing rapid response measures to ensure cybersecurity has required the development of an institutional system. The Government of the Republic of Moldova adopted the Resolution №. 414 of 08.05.2018 "On measures to consolidate data centers in the public sector and rationalize the administration of state information systems". The key decision of this decree was the reorganization and transformation of the state enterprise "Center for Special Telecommunications" into the Public Institution "Information Technology and Cyber Security Service". The implementation of the provisions of this Government Decree allowed, in a short time, to radically rebuild the entire cybersecurity infrastructure of the country, ensure a hierarchical line among various state bodies in terms of their responsibility for the development of information resources, and centralize the management of the telecommunications infrastructure with the creation of a single technological platform that provides electronic public services.

Two years later, the Cabinet of Ministers of Moldova was forced to adopt amendments and additions to this Decree to further specify the functions and responsibilities of the Information Technology and Cyber Security Service, as well as expand the list of measures that could be taken to ensure the cyber security of Moldova. By Government Decree № 482 of 08.07.2020 the "Measures necessary to ensure cyber security at the government level» were approved and amendments were made to Resolution № 414/2018. By this document, the Public Institution "Information Technology and Cyber Security Service" is designated as the Governmental Centre for Response on Cybersecurity Incidents. In addition, there were introduced a few more entities:

- The Governmental Centre for Response on Cybersecurity Incidents (CERT Gov) - an entity that serves as a single point of communication and reporting of cybersecurity incidents and has the necessary capacities to prevent, analyze, detect and respond to cyber incidents at the government level;

- The Departmental CERT - a subdivision or responsible person appointed within public entities that manages the infrastructure of information technology and communications and has the necessary capacity to maintain the mandatory operational records and reporting of cybersecurity incidents.

Cybersecurity laws and regulations in Moldova cover common issues in cybercrime, applicable laws, methods for preventing attacks, specific sectors, corporate governance, litigations, insurance, and investigatory and police powers in 26 jurisdictions. Protecting the national cyberspace against emerging cyber threats involves a long and complex process of planning and implementing of defensive measures.

Despite the fact that Moldova was able to establish the core of the national cybersecurity system, the activities of the main structures of Moldova's national cybersecurity system remain insufficiently coordinated and focused on performing current tasks. According to the results of expert assessments, the conditions of implementation of the National Cyber Security Program of the Republic of Moldova for 2016-2020, according to certain indicators, were not sufficient and some of the provisions had not been fully implemented. The issues related to the operative exchange of information on cyber threats, an effective training system and effective model of public-private partnership remain unresolved. The implementation of the National Cyber Security Program was complicated by the lack of a holistic vision for the development of capabilities of the main structures of the national cybersecurity system, the limited available resources that could ensure the functioning of this system, and the lack of proper government support for its institutional adaptation.

Indicators for the implementation of the National Cyber Security Program have not been developed, which has complicated the process of evaluating its effectiveness and identifying gaps and unfinished tasks. Academic research and public institutions were insufficiently involved in the development of the scientific potential of the cybersecurity field and the spread of cyber literacy. The list of critical information infrastructure has not been defined yet, and the model of functional public-private partnerships in cybersecurity has not been created. The development of the digital literacy was carried out without a clear program, and cyber learning was conducted sporadically.

There is an urgent need to recover the gaps identified in the previous stages. The spectrum of these policy failures should be taken into account by the current pro-European authorities when implementing the planned Government Action Plan for 2021-2022. Within this action plan, a special attention is paid to the reform and modernization of the security sector based on the national security interests of the Republic of Moldova and new challenges and threats to the national, regional and global security.

Another important issue is related to ensuring the democratic civil control over the functioning of the national cybersecurity system, namely the cybersecurity entities' compliance with the Constitution and laws of the Republic of Moldova, the state of and progress in the implementation of strategic documents, state programs and plans in this field, and the efficient use of resources, including budget funds. Law enforcement and specialized agencies with law enforcement functions should enhance capabilities to minimize the threat of cybercrime, and have their technological and human resources strengthened to ensure an efficient application of preventive measures and investigation of cybercrimes.

COOPERATION OPPORTUNITIES FOR THE ASSOCIATION TRIO TO STRENGTHEN THE CYBER RESILIENCE

For many years the EU has provided considerable input for the digital transformation of the EaP states. In the Joint Communication "The Eastern Partnership beyond 2020", one of 4 main pillars was dedicated to digital transformations and involves the establishment of a "Partnership that connects". Thus, the EU is going to invest further in the partner countries' digital transformations. A special attention is paid to the development of infrastructure, cybersecurity, and e-governance.[1]

The EU is currently implementing various projects and programs in this area for the period 2019-2022, which focus on cybersecurity development. Among them are *EU4Digital: Cybersecurity East; CyberEast - Action on Cybercrime for Cyber Resilience in the Eastern Partnership region; EU4Digital: supporting digital economy and society in the Eastern Partnership.* Given the development of artificial intelligence technologies that will continue to take place in the next years, the scale and consequences of such interventions will increase. The

[1] Digital transformation and cybersecurity: what is on the 2021 agenda in the EU and EaP?, https://www.euneighbours.eu/en/east/eu-in-action/youth/stories-young-european-ambassadors/digital-transformation-and-cybersecurity

cyber incident response capabilities of these countries should be adequately prepared for this new stage, which requires the ability to effectively deter destructive actions in cyberspace, achieving cyber resilience at all levels and ensuring the interaction of associated countries in cybersecurity through cooperation.

Considering the upcoming 2021 EaP Summit, there is a clear need for a greater emphasis to be put on cybersecurity within the future EaP agenda, and a deeper dialogue, especially with the EU and associated countries (Moldova, Georgia and Ukraine) in this regard. Cyberspace represents one of the possible military operating domains. There is an ongoing trend of developing new kinds of forces - cyber forces, which aim not only to protect the critical information infrastructure from cyberattacks, but also conduct preventive offensive operations in cyberspace. This requires the expansion of mutual collaboration in the framework of the "Association Trio", to improve the common defense and capacity-building measures.

In line with the establishment of a "European Cyber Shield" in the EU countries, it is important to improve the operational capacity of the "Association Trio" group to increase the degree and frequency of information exchanges between stakeholders and to provide timely warnings of cyber security incidents. Building a cybersecurity crisis management framework between associated countries will represent an important step in this direction.

COOPERATION OPPORTUNITIES FOR ASSOCIATION TRIO AND EU IN CYBERSECURITY

The expansion of the threats landscape and the complexity of the tools that could be used to address them encourage governments of leading countries to improve the architecture of national cybersecurity systems, and change the strategy and tactics of combating cyber threats. Changes are being made to the ways and means of countering cyber threats, while acknowledging the inability to build completely invulnerable and resilient security systems.

The EU sets digitalization and cybersecurity among its key priorities. To keep pace with today's digital transformations, the fundamental issues and processes within EU's strategy on cybersecurity are changing. In December 2020, the EU released its new Cybersecurity Strategy (EUCSS). The strategy identifies three dimensions of EU action and provides concrete proposals for regulatory, investment, and policy initiatives to safeguard a global and open internet, protect the European values, and improve resilience, technological sovereignty and operational capacity for responding to cyber incidents.[2] In the new Multiannual financial framework for 2021-2027, the digital sector is defined as a priority across programs. A minimum of 20% of the EU Recovery Package will be dedicated to the digital sector and digital transformations.[3]

The UE countries, NATO, leading international companies and experts unanimously recognize the Russian Federation and its actions in cyberspace as a major threat to international cybersecurity. Its cyber-exploration activities are part of the hybrid war that is waged against the EaP countries. The trends in Russian cyber activity over the past few years suggest that Kremlin is, and has been, significantly investing in developing its strategy, tactics, and tools to leverage cyber capabilities. Kremlin invests approximately $300 million per year to improve the offensive cyber forces and employs about 1,000 on-keyboard personnel.[4]

The EU countries do not want to antagonize the Russian Federation. This self-restraint creates a situation where the EU focuses on "soft issues" and Russia exploits hard security vulnerabilities. The EU itself prefers to speak about

[2] Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy, https://www.consilium.europa.eu/en/press/press-releases/2021/03/22/cybersecurity-council-adopts-conclusions-on-the-eu-s-cybersecurity-strategy/

[3] Infographic - Multiannual financial framework 2021-2027 and Next Generation EU, https://www.consilium.europa.eu/en/infographics/mff2021-2027-ngeu-final/

[4] Russia and Cyberspace, https://www.newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean/russia-and-cyberspace/

resilience rather than security. Five out of the six EaP countries are grappling with unresolved conflicts, territorial disputes, or non-recognized entities on their territory where Russian troops are involved. Georgia, Ukraine and Moldova demand more involvement of the EU in contributing to the settlement of their protracted conflicts.

In the last decade, the EU has ramped up its assistance to security sector reform in the EaP countries but has primarily focused on "soft security", most notably the prosecutors, the judiciary and the police. The EU has a growing range of instruments at its disposal, including the beefed-up EDF and the PESCO framework. In November 2020, ECFR published a proposal for the EU Security Compact, recommending the EU to mend its security ties with select Eastern Partnership countries.[5] The proposal deliberately includes issues of intelligence cooperation, both "soft" and "hard" security, and assistance to modernize the military hardware. It remains debatable whether or not the "Association Trio" itself is a suitable framework to engage in such security and defense cooperation. This issue requires more clarity and input from the EU.

RECOMMENDATIONS

Based on the above-made assessment on the reform achievements and policy failures in Moldova's cybersecurity space, certain steps are required to be undertaken, which might be useful for the public institutions' abilities to strengthen the national cybersecurity, ensure its resilience and defend the cyberspace:

- Moldova's national cybersecurity system should be based on permanence of measures to improve the legislation in this field and prompt actions to update it according to the changing security conditions, on a comprehensive understanding and analysis of the digital environment, including the global trends in the cybersecurity environment.

- The broad spectrum of cyber threats in Moldova's landscape showcases the need to identify clear roles, needs and responsibilities in solving cybersecurity issues and tasks of varying complexity, use incentives and exchange of knowledge and international experience in the field. The implementation of modern principles, integral methods, approaches and mechanisms of public administration in this field, including those based on strategic planning and management, crisis management, and partnerships between the state, the business environment and society, should take place with the optimal use of legislation, standardization, educational programs, mechanisms to stimulate and strengthen trust, and the exchange of information and best practices.

- The adaptation to this new reality has brought to light both the advantages of an innovative and robust public administration and the need for a thorough understanding and reassessment of the cybersecurity implications for both the EU and the "Association Trio" countries. This requires joint efforts to safeguard the cyberspace from illicit use and exploitation, and other related crimes, as well as promote the strengthening of the national cybersecurity through the strategic use of cybersecurity instruments. It is necessary to improve the common cyber defense capabilities, to face sophisticated and emerging cyber threats that may affect the military information networks, management and security.

- The lessons learned from the previous cases of cyberattacks need to be taken into consideration, in order to improve the resilience of critical infrastructure and ensure preparedness against such attacks. Given that Russia's actions in cyberspace are acknowledged as a major threat to the regional and international cybersecurity, it would be important for the associated countries to become part of the "European Cyber Shield". This is the only way to confront Russia's massive and destructive cyber activity in the region.

[5] Gustav C. Gressel EU Security Compact for the Eastern Neighborhood: Why unity of command is an issue in politics too European Council on Foreign Relations (ECFR). Clingendael Report. 2021, https://www.clingendael.org/pub/2021/the-eastern-partnership/annex-3/

ABBREVIATIONS:

CERT Gov - Governmental Centre for Response on Cybersecurity Incidents
EaP - Eastern Partnership
EDF- European Defence Fund
ENISA - European Union Agency for Cybersecurity
ECFR - European Council on Foreign Relations
EU - European Union
EUCSS - European Union Cybersecurity Strategy
ICT - Information and communication technology
NATO - North Atlantic Treaty Organization
NCPDP - National Center for Personal Data Protection of the Republic of Moldova
PESCO - Permanent Structures Cooperation
SIS - Security and Intelligence Service

ABOUT THE AUTHOR

Natalia Stercul is a political analyst, doctor of philosophy in political sciences, assistant professor, expert, Department of Eastern Studies: Ukraine and Russia, Foreign Policy Association of the Republic of Moldova. In its didactic practice, Natalia actively cooperates with nongovernmental agencies in Moldova and abroad, promotes development of the younger generation of leaders, by involving them in the international projects and socio-political processes. She was awarded a degree in public relations in the Moldova State University and the Academy of Sciences. Natalia Stercul is the author of a number of research papers and analytical papers.

STRENGTHENING THE NATIONAL CYBERSECURITY OF GEORGIA

by Irakli Jgharkava
Georgian Center for Strategy and Development

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 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,[6] and it is one of the most vulnerable areas of the country's security architecture. The Association Trio[7] 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[8] proved that Georgia is still far from

[6] Davit J. Smith, "*Russian Cyber Strategy and the War Against Georgia,"* Atlantic Council, Available at the following link (consulted on: 25.08.2021).
[7] 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).
[8] "*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).

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.[9]

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.[10] Since then, Georgia has repeatedly been the target of cyberattacks from Russia, including the large-scale attack from October 2019[11] 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,[12] 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.[13]

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

[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] *Ibid*
[11] "*Georgia hit by massive cyber-attack*," BBC, Available at the following link (consulted on: 30.08.2021)
[12] Andro Gotsiridze, Cybersecurity consultant, Cyber Security Studies & Education Center (CySec), Interview, August, 23, 2021.
[13] *Ibid*

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.[14]

According to the cybersecurity expert Vladimer Svanadze, 2017 was the most successful year for Georgia in the field 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.[15] 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.

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.[16] Yet, another ambiguity is the absence of the Single Point of Contact (SPoC) on cybersecurity matters, which is a serious problem;[17] 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.[18] 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.[19] The main goal of the newly formed alliance is to collectively find ways to speed up the membership in the European Union. 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.

[14] 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).
[15] Vladmier Svanadze, Director of Georgian Academy of Technological Innovations, Interview, August 23, 20221.
[16] "*Parliament Passes Controversial Information Security Laws*," Civil.ge, Available at the following link (consulted on: 31.08.2021).
[17] Giorgi Iashvili, Georgian Information Security Association, Interview, August 30, 2021.
[18] Vladmier Svanadze, Director of Georgian Academy of Technological Innovations, Interview, August 23, 20221.
[19] Vlagyiszlav Makszimov, "*Georgia, Moldova, Ukraine formalise their higher EU ambition,*" EURACTIV, Available at the following link (consulted on: 30.08.2021).

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 missions and operations, and participating in the EU Permanent Structured Cooperation projects.[20] 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 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

[20] „*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).

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, the U.S. National Institute of Standards and Technology, and the Information Systems Audit and Control Association. 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 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.

STRENGTHENING THE NATIONAL CYBERSECURITY IN UKRAINE

by Hennadiy Maksak
Foreign Policy Council "Ukrainian Prism"

SUMMARY

With the onset of the Russian military aggression on the territory of Ukraine, the cyber-space has appeared in the Russian-Ukrainian conflict as a new theater for waging warfare. Since 2014, Ukraine has become a cyber testing ground, where the Russian state-controlled hackers have been applying their malicious intrusions into the networks of public institutions, power grids and state enterprises.

The existing model of national cybersecurity has gone through several important phases. With the main cybersecurity elements being initially introduced back in the mid-2000s, the first thorough approach to constructing the Ukrainian cybersecurity architecture was considered and taken in 2016-2017. At that time, the National Cybersecurity Strategy was introduced, and subsequent legislation was adopted in the Ukrainian parliament. For all its flaws and shortcomings, the institutional and strategic levels of the current cybersecurity architecture have been set. The next critical phase in developing cyber capabilities started in 2020 and is still actively unfolding. In 2021, a new Cyber Strategy was approved, and new initiatives were taken in various areas connected to security in the cyberspace. Nonetheless, one cannot say that Ukraine has strong defense capabilities in cyberspace. There are outdated laws on data protection, a low level of interaction between state agencies and the business sector, and sometimes, an absence of clear measurable targets in this dimension.

As an important part of the enhancement of its cybersecurity, Ukraine considers international cooperation on multilateral and bilateral levels. To fight cybercrimes, Ukraine forged several memorandums and agreements with partners, including the US, NATO and the European Union. Some initiatives are implemented under the framework of the Eastern Partnership policy, which also poses a prospect of a close partnership for the Association Trio. In addition to that, the European Union is seen as a strategic partner in fighting cybercrimes and creating resilient critical infrastructure.

INTRODUCTION

In 2014, Ukraine appeared to be unprepared to the constant flow of Russian cyberattacks that sought to undermine Ukraine's key infrastructure and the functioning of its public institutions. Ukrainians experienced a wide array of cyber intrusions: DoS campaigns, website defacement, cyber espionage and attacks on vital public objects. A massive blackout in one of Ukraine's regions left hundreds of thousands of Ukrainian citizens without electricity. Achieving a high cybersecurity environment in Ukraine was not considered to be a trendy thing to do against the backdrop of constant military and hybrid aggression. The process for setting the proper legislative and institutional frameworks for cybersecurity was lengthy and sometimes incoherent.

In 2016, under President P. Poroshenko and his team, the *Cybersecurity Strategy* was adopted in Ukraine in line with the *National Security Strategy* (2015). A number of severe cyberattacks that hit Ukraine in 2017, has prompted further steps for protecting the country's critical infrastructure, in particular. In 2017, another framework, the *Law on Basic Principles of Cybersecurity* was passed in the Parliament. The General Requirements for Cybersecurity of Critical Infrastructure (2019) has also enriched the legal basis for cyber protection.

At the same time, the current cybersecurity architecture has appeared. The National Coordination Center for Cybersecurity (NCCC) at the National Security and Defense Council of Ukraine (NSDCU) was launched in 2016 under the framework of the Strategy of the Cybersecurity of Ukraine. It is presided by the Secretary of the National Security and Defense Council of Ukraine and consists of heads of the MOD, the General Staff, Security Service of Ukraine, National Police of Ukraine, intelligence agencies, the State Service of Special Communications and Information Protection of Ukraine. The NCCC acts as one of three situational centers, which monitor the processes that take place in the national security field. One cannot say that the activity of these agencies was set up and steered. At the same time, Ukraine managed not to fall victim to many serious "black-out" cyber assaults. A new cycle of developments in the field of cybersecurity started with the election of V. Zelenskiy in 2019. Our task is to look at the recent developments in the cybersecurity domain, as well as at Ukraine's international cooperation in cybersecurity-related areas and issues.

POLICY EVALUATION

The current context, risks, threats, challenges and priorities in the policy area

Under President Zelensky, the issue of digitalization was elevated to the top state priorities. The government and executive agencies have been tasked with advancing the project "The state in smartphone", which is focused on the digitalization of a vast number of services delivered by public institutions in Ukraine. Within the government, the Ministry of Digital Transformation was established in 2019. The Minister of Digital Transformation, M. Fedorov, vowed to bring online public services by 2024. This naturally drew attention to the importance of having a consistent and effective cybersecurity policy in Ukraine, both on the legislative and institutional level. It also revealed many sore spots in Ukraine's current cyberspace.

Cybersecurity has become an important field and issue on the country's international cooperation agenda with the EU, NATO, USA, Israel and many other partners. Ukraine is still in the process of translating and implementing the *Budapest Convention on Cybercrime* into its domestic legislation. In 2021, Ukraine initiated the first Cyberdialogue with EU and applied to the NATO center of excellence in cybersecurity. With that being said, all undertaken efforts have not resulted in a secure environment and sustainable cybersecurity architecture. The Global Cybersecurity Index (GCI), launched in 2015, positioned Ukraine on the78th place out of 194 states in 2020[21].

The major challenge to the political pledge of bringing the majority of public services online is the poor quality of existing public registers, their vulnerability to cyberattacks and the disruption operations led by Russia or any other malign hacker group. At the same time, these databases lack certain pieces of information or have multiple duplications of data. The insufficient number of specialists in this field, as well as the low level of competencies and specific skills-building and training, also aggravate the situation. The poor level of awareness of Ukrainian citizens about basic cyber protection rules creates a conducive environment for cybercrimes and abuses. This is applicable for both the public and private sector.

It is important to mention that Ukraine still preserves a negative leadership in terms of the number of cyberattacks it faces, initiated by Russian cyber terrorists, either state-sponsored or those with no direct connection to Kremlin. On a monthly basis, the cybersecurity unit of the Security Service of Ukraine prevents about 50 to 100 serious hacker attacks that are spearheaded on Ukrainian public institutions and objects of critical infrastructure.

[21] Global Cybersecurity Index 2020 Measuring commitment to cybersecurity, 2020, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

MAIN REFORM, POLICY ACHIEVEMENTS AND FAILURES IN THE POLICY AREA

Legislative and strategic documents base

Since 2020, the legislative base on cybersecurity has significantly improved. Thus, in September 2020, the new *National Security Strategy* was signed by the President of Ukraine. This document created preconditions for drafting a profile strategy for the cybersecurity domain. In October, a task force was created under the National Security and Defense Council of Ukraine. This group included core bodies of the national cybersecurity system, along with representatives of the Verkhovna Rada of Ukraine, the Office of the President of Ukraine, and profile government institutions (the Secretariat of the Cabinet of Ministers, the Ministry of Energy, the Ministry of Infrastructure).

In March 2021 the task force already approved the draft *Cybersecurity Strategy of Ukraine for 2021-2025*. Under the provisions of the documents, Russia remains as a dominant source of cyber threats for Ukraine. And cyberspace itself is acknowledged as a theater of war. In August 2021 with the Presidential Decree № 446/26.08.2021 the *decision of the NSDCU "On urgent measures for cyber defense of the state"* (14.05.2021) was enacted. With this Decree, the Cabinet of Ministers was tasked with preparing a draft law on the creation of cyber forces under the framework of the MoD of Ukraine, during a two months period[22].

Institutional framework

In January 2020, the functions of the NCCC were extended after the issuing of a Decree of the President of Ukraine. It helped to streamline the coordination of all profile agencies and enhance the cooperation with the private sector, which has been regarded as a long-standing weak chain in the cybersecurity of Ukraine.
To address the insufficient level of cooperation between the public and private sector in the field of cybersecurity, some contacts have been established by the NCCC in recent years.

In 2020, the NCCC arranged meetings with the US and Israeli companies in order to boost Ukraine's cyber defense capabilities. Such companies as Cisco, Fortinet, IBM, MicroFocus, Microsoft and Radware demonstrated their interest in cooperating[23]. In 2020-2021, the NCCC was active in establishing close cooperation with other governmental institutions and international organizations. Respective MoUs on cooperation in the cybersecurity field were signed between the NSDCU and the Ministry of Infrastructure of Ukraine, the Ukrainian Chamber of Commerce and Industry, IFES Ukraine.

Among the core public agencies involved in cyber protection are the State Service of Special Communications and Information Protection of Ukraine (SSSCIPU), the Security Service of Ukraine, and The Cyber Police Department. In May 2021, under the SSSCIPU umbrella, the Cybercenter UA30 was officially launched. The main task of the brand-new body is to provide cyber protection for public information resources, objects of critical infrastructure and the Ukrainian cyberspace at large. Within the toolkit of the Cybercenter UA30 there are legislative changes in the area of cybersecurity, international cooperation, capacity building and awareness-rising campaigns. More specifically, the Center UA30 will be focusing, firstly, on the protection of public registers, which are utilized by the app "Дія". It is planned to cover 80% of registers by 2024. Secondly, a priority will be the protection of Ukrainian citizens, private and corporate information. Thirdly, UA30 will be engaged in the promotion of cyber hygiene among Ukrainian citizens with a pledge for 95% of the country's

[22] УКАЗ ПРЕЗИДЕНТА УКРАЇНИ №446/2021, Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про невідкладні заходи з кібероборони держави", https://www.president.gov.ua/documents/4462021-40009
[23] Апарат РНБО України співпрацюватиме з найбільшими приватними компаніями у протидії кіберзагрозам, 14.02.2020, https://www.rnbo.gov.ua/ua/Diialnist/3916.html

population to master basic digital skills over the next three years. The fourth priority is to form a personnel reserve of cyber specialists.

For incidents response, there is the CERT-UA team in charge. It is the only state-sponsored group that is accredited in the FIRST (Forum of Incident Response and Security Teams) to provide assistance to public and private organizations and citizens. A first of its kind in Ukraine, the Training cybercenter has also been created within the framework of the new body, with advanced possibilities to test various scenarios of cyber threats (it was claimed that this training facility is among the 20 most advanced in the world)[24].

International cooperation and support

The United States stands as a strategic partner in the process of the development of the Ukrainian cybersecurity field. In 2020, USAID launched the project "Cybersecurity of Ukraine's Critical Infrastructure" with the aim to reduce the cybersecurity vulnerabilities in critical infrastructure and foster intersectoral cooperation among the government, private business, academia and civil society in the field of cybersecurity. The implementation period of this project is 2020-2024.

Within the established cooperation with CRDF Global (USA) under the support of the US State Department, the format of the *National cybersecurity cluster* was launched in February 2021. It envisages holding regular meetings to discuss cybersecurity issues in Ukraine under the umbrella of the NCCC. The main task is to boost the coordination efforts between public agencies, international donor organizations, foreign embassies and non-governmental sector[25]. This format became a wide forum for cyber-related discussions within the cooperation of the NCCC and CRDF Global (USA). To take stock of the first six months of the Cluster's operation and work, the first National Cybersecurity Summit was held in Kyiv in September 2021. It was attended by representatives of profile Ukrainian state agencies, MPs as well as diplomats from the United States, Great Britain, Estonia, NATO, OSCE and members of international organizations such as Sovereign Ventures, Salucyber DAI, IFES, etc.

Besides the robust US assistance for boosting the Ukrainian resilience in the digital field, cybersecurity stands as one of the priorities on the Ukraine-US intergovernmental agenda. Recently, it translated into a clear manifestation in the *Joint Statement on the U.S.-Ukraine Strategic Partnership*, the result of the visit of President V. Zelenskyy to Washington in September 2021[26]. This declaration demonstrates the existence of a common will to extend the cooperation in the cybersecurity domain, including on information exchange, as well as the US support for capacity building in the area of cybersecurity in Ukraine.

The 4th U.S.-Ukraine Bilateral Cyber Dialogue at the inter-governmental level is planned to be held. On the margins of President Zelenskyy's visit to the US, it was agreed that until the end of 2021, the State Service of Special Communications and Information Protection of Ukraine and the US Cybersecurity and Infrastructure Security Agency (CISA) will sign an agreement, devoted to many areas of cooperation in cyberspace. It refers namely to the exchange of experience on counteracting the cyber aggression of Russia, the elaboration of joint

[24] Перший кіберцентр в Україні. Як він захищатиме державу і кожного з нас?Навіщо в Україні створили кіберцентр, чим він буде займатися і чому кібербезпека стане трендом кількох наступних років, 14 May 2021, https://www.epravda.com.ua/columns/2021/05/14/673864/

[25] В Апараті РНБО України відбулася перша координаційна зустріч Національного кластеру з кібербезпеки, 26.02.2021, https://www.rnbo.gov.ua/ua/Diialnist/4826.html.

[26] *Joint Statement on the U.S.-Ukraine Strategic Partnership,* the result of the visit of Presidents V. Zelenskyy to Washington in September 2021. https://www.whitehouse.gov/briefing-room/statements-releases/2021/09/01/joint-statement-on-the-u-s-ukraine-strategic-partnership/

protocols of action, the launch of a platform for information sharing on cyber incidents, and the use of the US experience in state and private partnership in the cyber sector[27].

In August, Ukraine applied for membership in the NATO Cooperative Cyber Defense Center of Excellence, located in Estonia. This cooperation could enhance the Ukrainian capabilities in detecting and deflecting cyber threats. NATO's decision on the application is due to be issued until the end of 2021[28].

COOPERATION OPPORTUNITIES IN THE POLICY FIELD FOR ASSOCIATION TRIO

Attempts to boost the cooperation between the three states have been undertaken in the framework of other international regional organizations. Namely, in 2019 efforts were taken by the Ukrainian, Georgian, Moldovan and Azerbaijani sides to create a regional cybersecurity center. The idea has not yet materialized[29].

Out of the three partner states of the Association Trio, Ukraine leads the chart in the digitalization domain. Thus, the positive experiences and negative lessons-learned of the country may present an interest for Georgia and Moldova. If successful, the Ukrainian project "The state in smartphone" may be an interesting case that could be adapted in the partner states. It is directly connected to cybersecurity, whereby protection should be guaranteed to public registers and databases.

Cybersecurity is essential for bilateral tracks. For example, both Ukraine and Georgia are interested in strengthening their cybersecurity. This was stated in June 2021, during the visit of President S. Zurabishvili to Ukraine[30]. This point was reinforced in the Batumi Declaration of the Trio's heads of state, where cyber resilience is mentioned in regards to the strategic direction of regional security cooperation with the European Union[31].

COOPERATION OPPORTUNITIES IN THE POLICY FIELD FOR ASSOCIATION TRIO AND EU

The necessity to prevent and constantly deflect the growing number of cyberattacks from state-sponsored and independent hackers is of serious concern to the EU. In December 2020, the European Commission adopted the new cybersecurity strategy. The main aim of the document is to foster high-level protection of critical infrastructure from external interference. It might be seen as a window of opportunity for the Trio to start cooperating on several important initiatives in the digital area, with cybersecurity being an integral component. The gradual involvement in the EU's cybersecurity policy will certainly present for the Association Trio significant experiences on how to reveal and counteract the threats, and address with more efficacy supranational challenges that both Trio and EU itself face.

[27] State Service of Special Communications and Information Protection kicks off cooperation with the US CISA, 03 September 2021, https://www.kmu.gov.ua/en/news/rozpochinayemo-spivpracyu-z-agentstvom-z-kiberbezpeki-ta-bezpeki-infrastrukturi-derzhdepu-ssha-derzhspeczvyazku

[28] Ukraine's application to join NATO's CCDCOE to be considered this fall, 11.08.2021,https://www.ukrinform.net/rubric-polytics/3296204-ukraines-application-to-join-natos-ccdcoe-to-be-considered-this-fall.html

[29] Країни ГУАМ хочуть створити регіональний центр кібербезпеки, https://www.ukrinform.ua/rubric-polytics/2654317-kraini-guam-hocut-stvoriti-regionalnij-centr-kiberbezpeki.html

[30] Кібербезпека та Чорне море: Зурабішвілі назвала завдання України та Грузії на шляху до НАТО, 23.06.2021, https://www.ukrinform.ua/rubric-polytics/3269348-kiberbezpeka-ta-corne-more-zurabisvili-nazvala-zavdanna-ukraini-ta-gruzii-na-slahu-do-nato.html

[31] Декларація Батумського саміту, схвалена главами держав Асоційованого тріо – Грузії, Республіки Молдова та України, 19 липня 2021 року, https://www.president.gov.ua/news/deklaraciya-batumskogo-samitu-shvalena-glavami-derzhav-asoci-69609

Against this backdrop, the relevance of beefing up the public and private resilience in cyberspace is high on the agenda of EU and Associated partners. In pandemic times, the number of attacks launched against EU institutions and member-states has increased. It proves the necessity for more intensive information exchange and experience-sharing between the Association Trio and the European Union.

Ukraine may serve as a benchmark in keeping an active dialogue with the EU on cybersecurity-related issues. Ukrainian specialists have intensive cooperation with the European side in boosting the security of critical infrastructure in Ukraine against cyberattacks. Of particular importance was the interaction in the run-up and during the presidential and parliamentary elections in Ukraine in 2019. Joint efforts resulted in the effective protection of critical data, related to the processing of votes, which was a prime target of orchestrated attacks from the Russian side. Ukraine is also the first to launch technical negotiations with the EU on Cyber Dialogue. In January there was the first round of technical consultations between Ukraine and the EU, which were devoted to cyberdialogue preparation. In June 2021, the first Cyberdialogue between Ukraine and the EU took place in Kyiv[32].

HOW COULD EU AND MEMBER STATES ASSIST THE ASSOCIATION TRIO IN STRENTHENING RESILIENCE IN THE POLICY AREA

For the purposes of fostering cybersecurity capacities within the Association Trio, it might be instrumental to extend the positive experience of the EU-funded EU4DigitalUA project and initiatives, financed under its framework. With a budget of around 20.5 million EURO, EU4DigitalUA thematically covers the development of digital government infrastructure in Ukraine, public e-services, cybersecurity and data protection. Some initiatives are oriented on the sharing and transferring of experiences and practices.

For instance, in May 2021, in Kyiv, several cybersecurity exercises for representatives of Ukrainian state bodies took place. The exercises were carried out by the Estonian e-Governance Academy (eGA) in the premises of the newly established Cybercentre UA30, which houses a unique training center for Ukraine. Estonia is one of the most advanced states in the cybersecurity and e-governance fields, and its experience might be quite valuable not only for Ukraine, but equally for Georgia and Moldova.

CONCLUSIONS AND RECOMMENDATIONS

Digitalization is inevitable for the future development of the whole world, states and societies. Cybersecurity is a flip side of digitalization, towards which much attention must be paid. In order to minimize risks and prevent damages to national critical infrastructure, to protect their own citizens and businesses from deliberate negative intrusions, the authorities from the Association Trio countries should focus their attention on the following measures:

- To establish bilateral cyber dialogues of Trio partners and EU in order to align their cybersecurity practices with the European standards and best practices;
- To use all venues and frameworks within the EaP multilateral architecture related to digital and cyber issues for an exchange of experiences, and the initiation of joint training and information sharing fora for EU and Trio states;

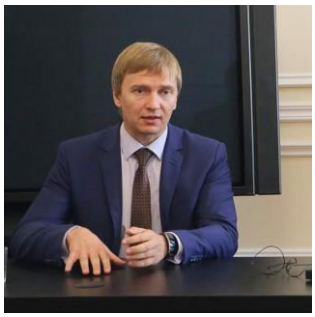
[32] Україна та ЄС започаткували Кібердіалог, 04 червня 2021 року, https://mfa.gov.ua/news/ukrayina-ta-yes-zapochatkuvali-kiberdialog

- To join the efforts of the Trio partner states to reveal Russian sponsored attempts to interrupt the work of public institutions in the three associated countries, share experiences and good cases for neutralization;
- Under the framework of a new horizon of the EaP deliverables until 2025 and available financial resources, to start joint training courses on cybersecurity for public servants in Georgia, Moldova and Ukraine. The assistance of the EU and US to relevant public agencies would be extremely important for raising the level of expertise in cybersecurity.
- It is critical to decentralize the cybersecurity efforts from capitals to the regions of the countries, which is a significant precondition for building a sustainable environment that could prevent cybercrimes.
- Comprehensive systems and mechanisms of nationwide, regional and sectoral cyber audits have to be introduced in all three partner-states, which would contribute to the mapping of objects of critical infrastructure and providing timely and efficient cyber protection.
- A specific form of cooperation might be established at the inter-parliamentary level to provide the necessary assistance to parliamentary bodies (committees, task forces, working groups) in the preparation and development of profile regulations for cyberspace. The Inter-parliamentary assembly Ukraine-Georgia-Moldova is a good platform to initiate this kind of experience-sharing.

ABBREVIATIONS:

CERT-UA - Governmental Centre for Response on Cybersecurity Incidents
CCDCOE - Cooperative Cyber Defense Center of Excellence
CISA - Cybersecurity and Infrastructure Security Agency
EaP - Eastern Partnership
eGA- e-Governance Academy
GCI -Global Cybersecurity Index
EU - European Union
FIRST - Forum of Incident Response and Security Teams
NATO - North Atlantic Treaty Organization
NCCC - National Coordination Center for Cybersecurity
NSDCU - National Security and Defense Council of Ukraine
MoD - Ministry of Defense
SSSCIPU State Service of Special Communications and Information Protection of Ukraine

ABOUT THE AUTHOR



Hennadiy Maksak is the Foreign Policy Council "Ukrainian Prism" Executive Director. Studied economics (Chernihiv state institute for economics and management), political sciences (Warsaw University, Center for East European Studies). In 2006-2015, he was the president of the Polissya Foundation for International and Regional Studies. In 2012-2014, 2017-2019 was a member of the Steering Committee of the Eastern Partnership Civil Society Forum. 2017-2021 was the Head of the Civic Council under the Ministry of Foreign Affairs. Fields of interest: International relations and foreign policy of Ukraine, Ukrainian neighborhood, Security in Eastern Europe, Eastern Partnership policy, diplomatic service.

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 theTransnistrian 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