Strengthening the national cybersecurity of the Republic of Moldova

EaP Security Forum

Natalia Stercul

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".

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.[1]

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[2], 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

[1] National Cyber Security Index, https://ncsi.ega.ee/country/md/
[2] Digital Report, https://digital.report/moldova-informatsionnaya-bezopasnost/

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 malware, 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.[3]

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.[4] 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.

RESILIENCE 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[5], 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.[6] One of the aims of the law was to ensure compliance with the EU Data Protection Directive 95/46.[7] 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".*[8]

[3]Cybersecurity of the Republic of Moldova: a retrospective for period 2015-2020, https://jss.utm.md/wp-content/uploads/sites/21/2021/03/JSS-1-2021_74-83.pdf

[4] The Court of Auditors' public databases were destroyed following a cyberattack, http://m.tvrmoldova.md/ro/social/bazele-de-date-publice-ale-curtii-de-conturi-au-fost-distruse-in-urma-unui-atac-cibernetic?fbclid=IwAR1Ec6oB17qpFbJeRmpBTnlNlNM8oa_LRkMZOiJ6UV2Fr-M2yqyMJigw60s

[5] Moldova has signed the Budapest Convention on Cybercrime (ETS 185) on 23 November 2001, ratified it on 12 May 2009 and it entered into force on 1 September 2009.

[6]Law № 133 on Personal Data Protection on 08.07.2011 (in 2020 this law was amended), https://www.legis.md/cautare/getResults?doc_id=121238&lang=ro

[7] EU Data Protection Directive 95/46, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046

[8] National Strategy for Information Society Development - Digital Moldova 2020, https://mei.gov.md/en/content/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.[9] 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,[10] 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*.[11]

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".*[12] 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"*[13] 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.

[9] National security. Analytical notes/ public policy proposals/ monitoring Institute of Public Policy September 2020, https://ipp.md/wp-content/uploads/2020/12/buletin-electronic-3-compres.pdf
[10] National Cyber Security Program of the Republic of Moldova for the years 2016-2020, https://mei.gov.md/sites/default/files/raport_evaluare_hg_811_2015_-_07.06.2021.pdf
[11] Cyber security, https://mei.gov.md/en/content/cyber-security
[12] Government Resolution of the RM № 414 "On measures to consolidate data centers in the public sector and rationalize the administration of state information systems "on 08.05.2018, https://www.legis.md/cautare/getResults?doc_id=122531&lang=ru
[13] Government Decree of the RM № 482 the "Measures necessary to ensure cyber security at the government level" on 08.07.2020, https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro

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.

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 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.[14] 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.[15]

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

[14] 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/

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

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.[16]

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 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.[17] 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

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

[17] 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/

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.

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 an author of a number of research papers and analytical papers.

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 officially 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