Strengthening the national cybersecurity in Ukraine

EaP Security Forum

Hennadiy Maksak

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.

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".

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 There are outdated laws on data protection, a low level of interaction between state agencies and the business sector, and sometimes, an absence of clear measurable targets in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 well 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[1].

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.

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

[1] 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

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[2].

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[3]. 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 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)[4].

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.

[2] 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

[3] Апарат РНБО України співпрацюватиме з найбільшими приватними компаніями у протидії кіберзагрозам, 14.02.2020, https://www.rnbo.gov.ua/ua/Diialnist/3916.html

[4] 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/

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[5]. 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[6]. 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 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[7].

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[8].

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[9].

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

[6] *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/

[7] 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

[8] 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

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

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[10]. 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[11].

COOPERATION OPPORTUNITIES IN THE POLICY FIELD FOR THE 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. 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[12].

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.

---

[10] 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

[11] 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

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

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

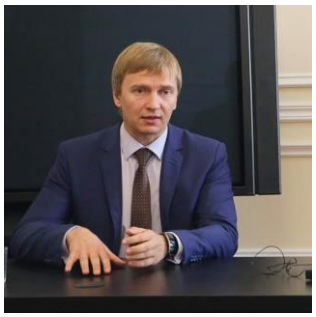
Digitalization is inevitable for the future development of the whole world, states and societies. Cybersecurity is a flip side of digitalization, towards which much attention must be paid. In order to minimize risks and prevent damages to national critical infrastructure, to protect their own citizens 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.
- 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 the Transnistrian conflict in the context of the country's Europeanization. APE was established in 2003 by a prominent group of local experts, public figures, former government officials and high-ranking diplomats, who decided to contribute throughtheir experience and expertise to the development of a coherent, credible and efficient foreign policy of the Republic of Moldova.

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

ABOUT THE PARTNERS ORGANIZATIONS

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

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

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

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