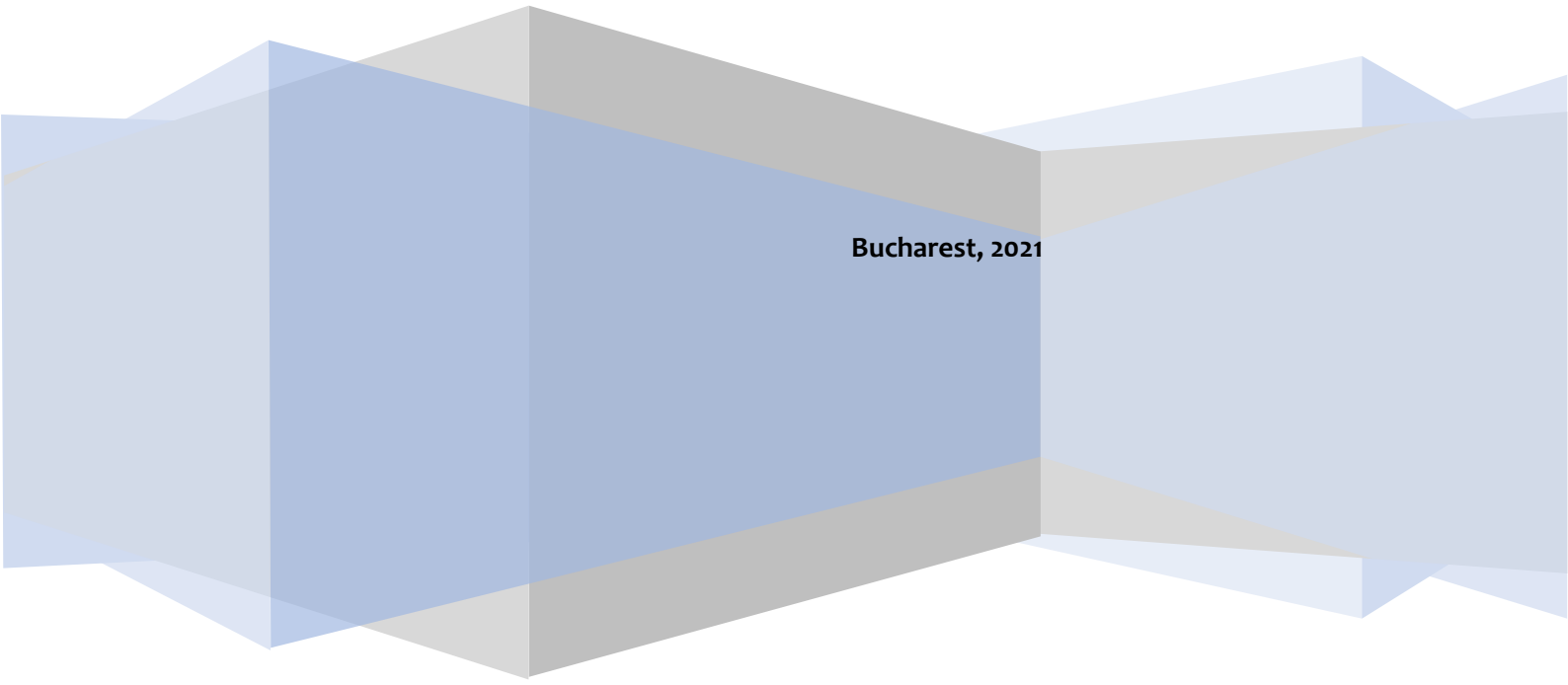
Experts for Security and Global Affairs

CYBER SECURITY IN THE CONTEXT OF UKRAINE - NATO COOPERATION

Policy brief

Sorin Bogdea



Bucharest, 2021

Abstract[1]

The formation of cybersecurity in Ukraine is considered in the context of modern challenges of information policy in a hybrid war. This paper analyses the evolution of cooperation in the field of cybersecurity between Ukraine and the NATO states and the diminishing vulnerability of Ukraine's cyberspace. The main purpose of the analysis is to define the role of strengthening international cooperation for the investigation of cybercrime that ensures the security of Ukrainian cyberspace. Ukraine's foreign policy efforts are aimed at involving international partners in ensuring the safe functioning of cyberspace. Such actions would strengthen the resilience of Ukraine's cyberinfrastructure and its ability to respond to potential risks. Tense relations with the Russian Federation regarding information and cyber dimensions have led to Ukraine's national cyber security system, which was intended to intensify cooperation with international partners in this field. The EU and NATO support Ukraine through joint programs in combating imminent threats. This creates the basis for a trilateral security partnership for strengthening stability in Europe in the context of ensuring security around Ukraine, with a long-term goal.

Keywords: informational security, countering hybrid threats, national cybersecurity system, cooperation, exchange of good practices

The Main Features of Cybersecurity

Cyberspace is defined as follows: "Cyberspace is a sphere of activity in the information space, formed by a set of communication channels of the Internet and other telecommunication networks, technological infrastructure that ensures their functioning, and any forms of human activity (personality, organization, state) carried out through their use" (Medeiros & Goldoni, 2020). Respectively, cybersecurity neutralizes threats to the availability, integrity, or confidentiality of data circulating in information systems. The problem of cybercrime is exacerbated by the lag of regulatory regulation in this area in Ukraine from the development of new information technologies. In order to coordinate and control the activities of various entities in the field of cybersecurity, the work of the relevant

[1] This policy brief is developed within the project "Romanian - Ukrainian Civil Society Forum for Dialogue and Cooperation. Third edition", implemented by the Experts for Security and Global Affairs Association, Romania, in partnership with Strategic and Security Studies Group and Foreign Policy Council "Ukrainian PRISM ", Ukraine, with the support of Black Sea Trust for Regional Cooperation, a project of German Marshall Fund. The views expressed in this policy paper are those of the author and do not necessarily coincide with those of ESGA partners.

public services has been organized, which have specific obligations to comply with cybersecurity requirements.

The first feature of cybersecurity covers information as an object of protection, not exclusively technical means that determine the possibilities for the functioning of information, but the protection of the ways of functioning of a new entity - cyberspace. In addition, cybersecurity is defined as one of the critical areas of national security by art. 3 of the Strategy of National Security of Ukraine. It recognizes cybersecurity and information security as one of the main priorities in combating threats to national security. Details of the Cyber Security Strategy implementation are reflected in the government's annual plans, which provide the authorities with measures to prevent and prepare to respond to possible cyber incidents within creating an effective national cybersecurity system. In the fall of 2015, as part of the reform of the Ministry of Internal Affairs in Ukraine was created a special unit - the cyber police, which is designed to protect citizens and the state from encroachments in cyberspace. The spectrum of his work is quite wide: police officers are involved in the fight against viruses, banking fraud and neutralization of pirated content.

The second feature is related to the organized activity of the Cyber Police Department of the National Police of Ukraine, specializing in the prevention, detection, cessation, and detection of crimes, preparation mechanisms, committing or concealing involving the use of computers, telecommunications, and computer networks and systems (Streltsov, 2017). As noted in a message on the Cyberpolice website[2], in 2020 it conducted 10 international police operations to expose hacker groups, detained 326 online fraudsters and stopped 62 facts of breach of intellectual rights.

After the Euromaidan protests, the number of cyberattacks against Ukraine increased. Due to the vulnerability of the informational sector, National Security and Defense Council of Ukraine (Рада національної безпеки і оборони України)[3] agreed to measures to protect state institutions.

National and regional context. Why cyber defence is important for Ukraine?

In early December 2014, NATO foreign ministers approved the launch of five trust funds to assist Ukraine in defense reform, which was decided at the NATO Wales Summit in early September in response to actions by the Russian Federation in Crimea and eastern

[2]https://en.interfax.com.ua/news/general/721768.html

[3]It is a state agency tasked with developing and coordinating a policy of national security on domestic and international matters in advising the President of Ukraine. The main functions are: Coordination and control over the activities of the executive bodies in the field of security and national defense in peacetimeand in case of crisis situations that threaten the national security of Ukraine.

Ukraine. It is estimated that the volume of each of these funds for military reforms in Ukraine should reach 1 million euros (Bağbaşlioğlu, 2016). The first trust fund refers to the modernization of communication systems and the automation of the Ukrainian Armed Forces according to modern standards, the second being intended for the retraining and social adaptation of military personnel participating in counterterrorism operations in Ukraine. According to Walt, who defines NATO's persistence after the Cold War as "something of an anomaly", the crisis in Ukraine is significant, as it becomes an opportunity to strengthen the alliance to act together (Walt, 2014).

The third will fund physical rehabilitation programs for wounded soldiers in Ukraine; fourth - provides for the reform of logistics systems and the standardization of the Armed Forces of Ukraine; and, finally, the fifth NATO Trust Fund is designed to combat cybercrime following the most progressive standards of NATO member countries. Considering Romania's experience in cyber defense, the North Atlantic Alliance trained Bucharest to lead the process of ensuring the protection of Ukrainian cyberspace. In this regard, the Minister of Foreign Affairs of Romania, Bogdan Aurescu, stated: "*At the summit in Great Britain, Romania expressed its readiness to lead this fund for the cyber defense of Ukraine*" (*Wales Summit Declaration*). At the Regional Summit in Bucharest in May 2015, Bogdan Aurescu emphasized the relevance of the regional geopolitical context on regional cyber security, and implicitly on Romania, as a "leading state" for the NATO-Ukraine Cyber Security Trust Fund.

On 3 August 2021, the delegation of the National Coordination Center for Cybersecurity of Ukraine during a working visit to the Republic of Estonia has submitted a request to join the NATO Cooperative Cyber Defence Centre of Excellence.The center is NATO accredited, it has a significant impact on the actions of the Alliance in the field of cyber defense. Seven countries founded the center, and today it has 20 members – 17 NATO members and three partner countries. Although it is not part of the NATO Command Structure, the Centre offers recognized expertise and experience in cyber defense. The centre's uniqueness lies in military, civilian, and representatives of the authorities work together there. According to Natalia Tkachuk, chief of the Information Security Office at the National Security and Defense Council "Membership in the organization will provide Ukraine with the opportunity to exchange experience in detecting and countering modern cyber threats, developing skills in a joint response to cyber-attacks and conducting defense and deterrence

operations in cyberspace."[4] Estonian Ambassador for Cyber Diplomacy to Estonian Ministry of Foreign Affairs Heli Tiirmaa-Klaar reconfirmed Estonia's support for Ukraine "*It is important for us to express this support in practical terms, and cybersecurity is one of the areas where the exchange of experience brings invaluable benefits to both parties*."[5]

Ukraine develops its cyber defence strategy to protect computer networks and cybercrime counteracting, oriented on the NATO model and strengtheningits information security. In response to large-scale attacks in recent years, the Defense Council of Ukraine approved the draft Cybersecurity Strategy of Ukraine for 2021-2025 (*Cybersecurity Strategy of Ukraine for 2021-2025*)

Legal norms aimed at ensuring national cyber security as a priority for implementing Ukraine's national policy have the character of public law and constitute an intersectoral legal institution. The basis of the administrative and legal status of the National Police in terms of cyber security today is the Law of Ukraine "*On Basic Principles of Cyber Security of Ukraine*"[6]. An important step towards the creation of a modern cyber security system in Ukraine was the adoption of the Resolution of the Cabinet of Ministers of Ukraine № 518 of June 19, 2019 "*On approval of General requirements for the cyber security of critical infrastructure*"[7],which established: definition of general requirements for cyber security critical infrastructure; establishing mandatory measures to ensure protection against cyberattacks; prevention of breach of confidentiality; integrity and availability of information resources; sustainable operation.

Assistance to Ukraine

Many international organizations have supported Ukraine to strengthen the resilience of critical infrastructure elements to cyberattacks. Albania, Estonia, Hungary, Poland, Portugal, Romania and Turkey have offered to contribute (financially or logistically) to the Cyber Defense Fund of Ukraine, a program agreed by the world's leading leaders at the September NATO Summit in Wales.

[4]Ukrinform, Заявку України про приєднання до Центру кібероборони НАТО розглядатимуть восениhttps://www.ukrinform.ua/rubric-polytics/3296159-zaavku-ukraini-pro-priednanna-do-centru-kiberoboroni-nato-rozgladatimut-voseni.html

[5]Officialpressreleasehttps://vm.ee/en/news/cybersecurity-elections-discussed-cyber-consultations-estonia-and-ukraine

[6]Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" https://zakon.rada.gov.ua/laws/show/2163-19#Text

[7]https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF?lang=en#Text

In particular, in 2014, Romania led the creation of the NATO Cyber Security Trust Fundand tapped the state-owned RASIROM company, one of the cyber-security providers for Romania's strategical state institutions. As part of this initiative, Ukraine received cyber capabilities exclusively for defense purposes and technical equipment for responding to cyberattacks and their further study. Since 2014, Ukraine has cooperated with Romania in the fight against hackers, phishing, and DDoS[8] attacks - which try to deactivate a site by overloading it with traffic.

The Cyber Defense Trust Fund for Ukraine aims to provide Ukraine with the necessary assistance to develop technical capabilities of defensive type, response to cyber security incidents, including laboratories for investigating cyber security incidents. (Cocolan, 2018)

Through bilateral relations, cybersecurity cooperation has also focused on providing Ukraine with logistical assistance to strengthen resilience to cyberattacks. Assistance includes establishing two Incident Management Centres to monitor cyber events and laboratories to investigate and handle cyber security incidents. With the support of the NATO Trust Fund, Situation Centers have been established under the Security Service of Ukraine, which are tasked with detecting, preventing and neutralizing cyber actions against Ukraine.

Due to this, the National Police of Ukraine has a 24/7 National Contact Point for Response and Exchange of Information on Computer Crimes. In order to strengthen the resilience of critical national cybersecurity infrastructure, the Ukrainian Government regularly participates in international cooperation in responding to cyber incidents, having access to international best practices and modern algorithms for responding to cyber incidents. It is the development of international cooperation in cybersecurity, participation in confidence-building measures in cyberspace under the auspices of the OSCE, and deepening cooperation between Ukraine and the EU and NATO that strengthen Ukraine's cybersecurity capabilities and meet national interests.

In 2017, the United States provided Ukraine with $ 5 million for cybersecurity needs, which included strengthening the resilience of electoral systems and critical infrastructure, supporting the implementation of the National Cybersecurity Strategy, and disseminating information on cybersecurity. In 2018, the US State Department doubled the amount of this assistance. ("Politico", 2019)

[8]A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure

Conclusions

The analysis showed that the problem of effective cybersecurity requires a comprehensive and continuous application of organizational, legal, and technical protection methods at different levels of implementation. The active phase of confrontation between the polar systems of collective security (alliances) in international cyberspace is still ongoing, encouraging NATO and the EU to develop a new strategic approach to preventing information aggression by Russia. The Ukrainian foreign policy vector should be aimed at intensifying joint action in the field of cyber security, continuing with the active participation of Ukrainian authorities and relevant NATO bodies through synergy, implementation of NATO information and technological standards in Ukraine, technical development capabilities of joint actions of Computer Emergency Response Team to cyber incidents.

In modern realities, the political leadership of Ukraine faces an important and responsible task: borrowing the best foreign experience, together with the world community to intensify the implementation of effective measures to combat international cybercrime, cyberterrorism, which primarily involves building an adequate model, efficient protection of national and informational resources and their critical infrastructure, approval of official accreditation by NATO of the National Center for Cyber Defense and Counteraction to Cyber Threats in order to develop a constructive cooperation with the NATO. The EU and NATO are interested in the space of peace and stability within Ukrainian territory that will guarantee their security.

According to international experience, national cybersecurity depends on implementing constructive measures to form a balanced state information policy, create reliable protection of critical information infrastructure and the internal segment of cyberspace, and integrate into global collective security systems, which requires a clear format. Under such conditions, the strategic task remains to improve the cyber security system that meets the criteria for Ukraine's accession to NATO. This actions the need to scientifically determine the activities of the state's political leadership to form the basis of international cooperation in cybersecurity in the current aggressive policy of the neighbouring country, creating mechanisms for rapid response to any cyber threats within the collective security system.

Bibliography:

1. Bağbaşlioğlu, A. (2016). THE IMPLICATIONS OF THE UKRAINE CRISIS FOR NATO SOLIDARITY: NATO BETWEEN COOPERATIVE SECURITY AND COLLECTIVE DEFENCE. *HititÜniversitesiSosyalBilimlerEnstitüsüDergisi*, *9*(2). https://doi.org/10.17218/hititsosbil.280809
2. Cocolan, M.-M. (2018). *International cooperation for Critical Information Infrastructure Protection: NATO-UKRAINE Trust Fund on Cyber Defence*. https://www.cipre-expo.com/wp-content/uploads/2018/10/Cocolan%20M%20NATO-UKRAINE%20Trust%20Fund%20on%20Cyber%20Defence.pdf, accessed 9thof November 2021;
3. *Cybersecurity Strategy of Ukraine for 2021-2025*.https://www.rnbo.gov.ua/en/Diialnist/4838.html, accessed 9thof November 2021
4. Medeiros, B. P., & Goldoni, L. R. F. (2020). The Fundamental Conceptual Trinity of Cyberspace. *ContextoInternacional*, *42*(1), 31–54.
5. Politico. (2019). *How Ukraine Became a Test Bed for Cyberweaponry*. https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/accessed 11thof November 2021
6. Streltsov, L. (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments. *European Journal for Security Research*, *2*(2), 147–184. https://doi.org/10.1007/s41125-017-0020-x
7. *Wales Summit Declaration*.http://www.mae.ro/sites/default/files/file/2014/pdf/2014.09.06_declaratie_summit.pdf , accessed 11thof November 2021
8. Walt, S. M. (2014). *NATO Owes Putin a Big Thank-You*. Foreign Policy, https://foreignpolicy.com/2014/09/04/nato-owes-putin-a-big-thank-you ,accessed 12th of November 2021

Bucharest, Romania

2021

www.esga.ro

Diaconu Coresi Str., nr. 53, Bucharest, Romania
Web: www.esga.ro, E-mail: contact@esga.ro