KONRAD ADENAUER STIFTUNG

Strategy XXI Стратегія

SYNERGING ENERGIES
Centre for Global Studies / Центр Глобалістики

Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the Cyber Sphere

Kyiv, 2019

KONRAD ADENAUER STIFTUNG

Strategy XXI Стратегія

SYNERGING ENERGIES
Centre for Global Studies / Центр Глобалістики

Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the Cyber Sphere

Kyiv
2019

Ukraine – EU – NATO Cooperation
for Countering Hybrid Threats in the Cyber Sphere

The analytical paper contains a comparative analysis of the regulatory framework, institutional capacity and level of activity to counter hybrid threats in the EU, NATO and Ukraine in the cyber sphere, as well as an assessment of the current state of cooperation between the EU and NATO and both organizations with Ukraine in the field of cybersecurity. Based on the analysis of the current challenges and threats in the cyber sphere and the forecast of their transformation taking into account the further aggressive intentions of the Russian Federation in the context of holding the presidential and parliamentary elections in Ukraine and the elections to the European Parliament, the formats of possible development of Ukraine’s cooperation with the EU and NATO in the field of cybersecurity are described.

The analytical paper was prepared by the Centre for Global Studies “Strategy XXI”, headed by President Mykhailo Gonchar and with the active participation of the Executive Director Vitalii Martyniuk, with the support and in cooperation with the Konrad Adenauer Stiftung Office in Ukraine. This initiative was launched with the European Neighbourhood Council (Brussels). The content of the paper is the responsibility of the Centre for Global Studies “Strategy XXI” and it does not necessarily reflect the vision of the Konrad Adenauer Stiftung.

© Centre for Global Studies “Strategy XXI”

CONTENT

Introduction 4

I. Regulatory and institutional framework of cybersecurity in the EU, NATO and Ukraine 5

II. Cooperation of Ukraine with the EU and NATO for cybersecurity 14

III. New cyber challenges and threats 19

IV. Strengthening Ukraine’s interaction with the EU and NATO in countering cyber threats 25

Conclusions 27

Introduction

Modern threats in Europe that emerged after the beginning of Russia's aggression against Ukraine in 2014 are relevant not only for Ukraine, but also for other countries that are members of the EU and NATO or those, which have taken a course towards membership of these organizations. This is evidenced by the final declarations of NATO summits, starting from Wales, and the EU Global Strategy and other strategic documents that have introduced the definition of "hybrid threats". Among these threats, disinformation campaigns focusing on splitting in countries and unions and interventions in information and computer systems are paramount.

Ukraine and the EU and NATO have turned out to be in a certain interconnection, when Ukraine cannot stand against Russia's current threats without international support, and the EU and NATO are interested in an area of peace and stability within the Ukrainian territory that would guarantee their own security. This creates the basis for a trilateral security partnership to strengthen stability in Europe in the context of ensuring security in and around Ukraine with a long-term goal of providing regional stability, peace and prosperity.

Ukraine already has some experience in confronting hybrid threats. It is in Ukraine that the Kremlin is testing new methods and means of conducting a hybrid war. However, the lack of sufficient resources and means to resist the aggression of Russia increases the importance not only of political support of the EU and NATO on the international scene, but also practical assistance in developing Ukraine's ability to confront these modern threats. In this context, cybersecurity has been at the heart of Ukraine – NATO – EU cooperation. It has been included in the list of seven key areas of NATO-EU security cooperation identified in the Joint Declaration on EU-NATO cooperation, become a priority for both organizations to help strengthening Ukraine's ability to guarantee its own security.

The field of cybersecurity clearly demonstrates the security interdependence of Ukraine, the EU and NATO. Technically, Ukraine needs help and support from both organizations, but the Ukrainian institutions that are responsible for this area are also getting unique experience in counteracting new threats that is of interest to Euro-Atlantic partners. Ukraine has become a landfill for Russia to test new ways and means of cyber warfare. Russian cyber activities are activated during the presidential and parliamentary elections in Ukraine. It is possible that certain technologies "run" in the Ukrainian elections will be used in the elections to the European Parliament. Therefore, such tripartite cooperation becomes especially relevant.

I. Regulatory and institutional framework of cybersecurity in the EU, NATO and Ukraine

The European Union is not a security alliance, although it has its own Common Security and Defence Policy, it was created as an economic union, and security for it is in both internal and non-military dimensions, and the counteraction to the hybrid threats is becoming particularly relevant there. Therefore, cybersecurity is one of the security pillars of today's security of the EU, and it had been put into priority areas much earlier than the definition of "countering hybrid threats" emerged in the EU terminology, especially given the active development of the digital market and the prospect of the creation of the "Digital Union of the EU".

Back in 2001, the European Commission adopted the Communication called Network and Information Security (NIS): Proposal for a European Policy Approach. Later, in July 2016, the EU approved the Directive on the safety of networks and information systems (NIS directive - Directive (EU) 2016/1148). According to it, the EU member states had to approve the relevant national laws by May 9, 2018 and identify the operators of key services in this area until November 9, 2018.

Although in the 2003 European Security Strategy, cyber threats were not included in the list of threats to the EU security, but cybersecurity reports were increasingly focusing on its implementation. As a conceptual document, in 2006, the EU approved the Strategy for a Secure Information Society.[1] Henceforth, cybersecurity becomes an integral part of the security documents of the European Union. In 2009, the Communication on Critical Information Infrastructure Protection (CIIP) was approved, and in February 2013 - the EU Cyber Strategy. The Global Strategy for the EU Foreign and Security Policy, endorsed in June 2016, has become the basis for the development of other sectoral and operational documents. There, cybersecurity is introduced into a separate security area, which includes the development of technological capabilities for countering cyber threats, reducing cybercrime, enhancing the stability of critical infrastructure, networks and services.[2]

Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace[3] determines the following EU strategic priorities: cyber resilience, cybercrime decrease, development of possibilities and policies for cyber protection, industrial and technological resources for cybersecurity, consequent international policy on cyberspace. In September 2017, the EU complements this Strategy, endorsing the Joint Communication of the European External Action Service and the European Commission on the Development of Proper Cybersecurity of the

[1] http://ec.europa.eu/information_society/doc/com2006251.pdf

[2] 87 per cent of Europeans regard cyber-crime as an important challenge to the EU's internal security, and in 2016, 80 per cent of European companies had at least one case of cyberattacks.

[3] https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

EU.[4] This document identified a package of additional measures aimed, first of all, at strengthening the EU Cybersecurity Agency (ENISA), establishing a common cybersecurity certification scheme for the EU, developing a response plan to large-scale cyberattacks and incidents, and strengthening research.

At the end of 2017, the Permanent Structured Cooperation on Defence (PESCO) was launched in the EU, with 25 of the 29 EU member states. One of the areas of this cooperation is cybersecurity, in particular, the creation of the Cyber Rapid Response Teams began. A positive decision for Ukraine is that third countries can be invited to participate in some PESCO projects, including cyber defence.

In December 2018, the European Parliament, the European Council and the European Commission reached a political agreement on the Cybersecurity Act [5], which also reinforced the mandate of the EU Agency for Cybersecurity, (European Union Agency for Network and Information and Security, ENISA), establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services.

The institutional dimension of the cybersecurity of the EU should be outlined. In 2004, the European Commission approved the decision to establish the ENISA Agency, which was planned to be transformed into the EU Cybersecurity Agency to assist EU member states in countering cyberattacks. The corresponding proposal was made by President Jean-Claude Juncker on September 13, 2017: "*Europe is still not properly equipped when it comes to cyberattacks. That is why today the Commission is proposing new instruments, including the European Cybersecurity Agency, to help our protection against such attacks.*" The agency should conduct an annual Pan-European cybersecurity training and exchange intelligence on cyber threats through the creation of Information Sharing and Analyses Centres. Another important function of the Agency was the certification of software products to meet the requirements of cybersecurity in the EU.

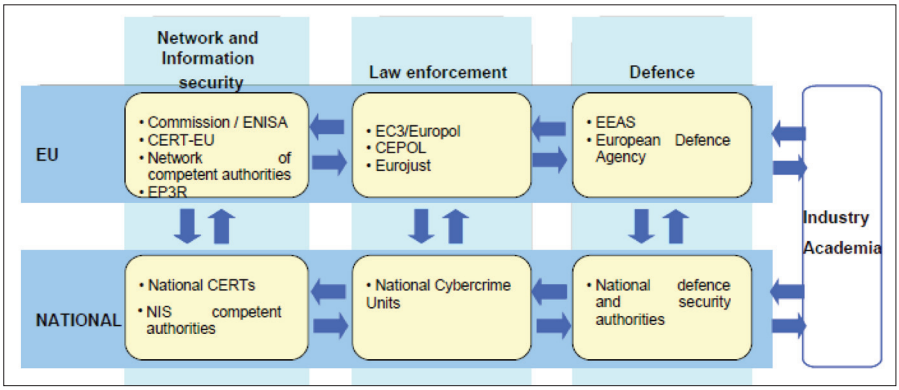
At the same time, the European Commission proposed the creation of a Cybersecurity Emergency Response Fund, to which the EU member states could join as desired. However, launched in late 2017 under the PESCO security initiative, the European Defence Fund, which, among other things, accumulated financial resources for cyber defence projects, actually put aside the need for a separate EU cyber fund.

In 2012, the Computer Emergency Response Team (CERT-EU) was created in the EU, which is responsible for the security of information systems of the EU institutions. The NIS Cooperation Group was set up under Directive 2016/1148/EU, which provided functions for strategic cooperation and exchange of information between member countries on cybersecurity issues. The Group directly coordinates the Network of Computer Security Incident Response Teams.

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=EN

[5] https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

In September 2018, the European Commission approved a decision to establish a network of competence centres in the member states, coordinated by the European Centre for Cybersecurity Research and Competence, which will promote the development of tools and technologies for countering cyber threats. In order to increase the involvement of the private sector in countering cyber threats, the European Public-Private Partnership for Resilience was established in the EU. The European Cybercrime Centre (EC3) operates within the framework of Europol.



Pic.1. The scheme of the EU cybersecurity institutions

In addition to very specific EU agencies, such as the abovementioned, Europol, Eurojust, the European Police College, European External Action Service, and the European Defence Agency (EDA), which already develop and coordinate common EU member states measure, are also responsible for cybersecurity issues. *"No country can face cybersecurity challenges alone. Our initiatives strengthen cooperation so that EU countries can tackle these challenges together. We also propose new measures to boost investment in innovation and promote cyberhygiene"*, - these words of Andrus Ansip, Vice-President for the Digital Single Market, demonstrate that official Brussels is increasingly teaming up to counteract cyber threats. [6]

Unlike the EU, in **NATO**, the counteraction to cyber threats is defined by the notion of *cyber defence*[7], which is included in the list of the core tasks of collective defence, which emphasizes its defence orientation, and not internal security, as in the case of the EU. NATO Secretary General Jens Stoltenberg clearly outlined three areas in this field: *"Today, NATO has three key roles to play in cyberspace. To drive progress across the Alliance. To act as a hub for information sharing,*

[6] http://europa.eu/rapid/press-release_IP-17-3193_en.htm

[7] https://www.nato.int/cps/en/natohq/topics_78170.htm

training and expertise. And to protect our networks".[8] Therefore, NATO focuses on protecting its own networks and strengthening the internal stability of its Allies, which is also relevant for Ukraine.

For the first time, the cyber defence was placed on the political agenda of the Alliance at its Prague summit in 2002. At the 2014 Wales Summit, NATO approved an enhanced cyber defence policy and an appropriate action plan for its implementation. This policy defined the activities of the Alliance in areas of awareness, education, training and exercises. At the same time, the counteraction to cyber threats was introduced under Article 5 of the North Atlantic Treaty[9], which is a very important decision, since a cyberattack on one country has an impact on the whole NATO. At the Warsaw Summit in 2016, the Alliance focused on strengthening the cyber defence of national networks and industries. At the same time, NATO mandate for operations in cyberspace, which equated to other areas of operations - land, air and seas, was confirmed. At the Brussels Summit in 2018, cyberattacks are among the main hybrid threats.[10] NATO agreed on the need to bring the operations of the cyber defence to the level of operations in the other three areas, both in the overall coordination of the Alliance and within the framework of separate groups of Allies.

The North Atlantic Council is putting into practice the overall implementation of the NATO Cybersecurity Policies. The Cybersecurity Committee, which manages the cybersecurity policy, is under its subordination. At the operational level, the NATO Cyber Defence Management Board (CDMB) is responsible for coordinating cyber defence activities between various NATO institutions and member states. This body includes senior political, military, operational and technical authorities of the Alliance, who are responsible for cyber defence. NATO also has got the NATO Consultation, Control and Command (NC3) Board and other bodies responsible for various issues of the cyber defence.

The Alliance operational bodies in the field of cybersecurity are:

- the Cyberspace Operations Centre, created by the 2018 Brussels Summit Declaration;

- the NATO Computer Incident Response Capability Centre (NCIRC) – performs the task of protecting NATO networks and provides centralized round-the-clock support to Allied computer resources;

- the NATO Cyber Rapid Reaction teams are constantly ready to assist Allies.

[8] https://www.nato.int/cps/en/natohq/opinions_154462.htm

[9] https://www.nato.int/cps/en/natohq/opinions_145415.htm?selectedLocale=en

[10] https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=uk

An important role is played by the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE), founded in 2008 and located in Tallinn, Estonia, which conducts research, training and exercise in cybersecurity, as well as the NATO Communications and Information Systems School (NCISS), NATO School in Oberammergau in Germany and the NATO Defence College in Italy, which serve for preparation of cyber defence specialists.

The concept of *"cybersecurity"* forces the Alliance to constantly expand its scope and means to counteract cyber threats, as indicated by the decisions of NATO and its bodies involved in this clash. In particular, it is increasingly interacting with industry and the private sector. To do this, the NATO Industry Cyber Partnership program has been developed and implemented. At the same time, NATO develops close cooperation with the EU and partner countries, including Ukraine, helping them achieve their two goals - protecting their own networks and strengthening their capabilities to counter cyber threats.

Ukraine develops its own cybersecurity in the areas of protection of computer networks and cybercrime counteracting, oriented on the EU model, and strengthens its cyber defence like the Alliance does it. Their relevance was confirmed in 2018 when Ukrainian cybersecurity specialists managed to block about 400 cyber-attacks. Some of them, according to the SSU (Security Service of Ukraine), could have had the consequences not less than the results of the Petya-A virus.[11]

Prior to Russia's aggression in 2014, Ukraine had already had a certain legal and regulatory framework in the field of cybersecurity. Thus, the International Convention on Cybercrime was ratified by the Law of Ukraine of September 7, 2005. Later, Ukraine began to revise and improve national legislation on cybersecurity. Russian aggression accelerated this process.

The 2015 National Security Strategy of Ukraine contains a separate block on cyber threats to the national security - "Threats to cybersecurity and security of information resources".[12]

According to the Strategy, the list of actual threats, carried out by Russia "for the exhaustion of the Ukrainian economy and undermining of social and political stability with the aim to destroy the state of Ukraine and seize its territory", includes threats to the cybersecurity and security of information resources:

- vulnerability of objects of critical infrastructure, state information resources to cyber-attacks;

[11] https://www.ukrinform.ua/rubric-technology/2638599-v-ukraini-torik-zablokuvali-majze-cotiri-sotni-kiberatak.html

[12] https://zakon.rada.gov.ua/laws/show/287/2015

- physical and moral obsolescence of state secret protection system and other types of information with restricted access.[13]

The main directions of the state policy of the national security of Ukraine include a special section called "Providing cybersecurity and security of information resources". The priorities for providing cybersecurity and security of information resources are defined as follows:

- development of a state information infrastructure;

- creation of a cybersecurity system, development of the Computer Emergency Response Team (CERT);

- monitoring of cyberspace in order to detect, prevent and neutralize cyber threats in a timely manner;

- development of law-enforcement agencies' capacities to investigate cybercrime;

- ensuring the protection of objects of critical infrastructure, state information resources from cyber-attacks, avoiding the use of software, in particular antivirus programs, developed in the Russian Federation;

- reforming the system of protection of state secrets and other restricted information, protection of state information resources, e-government systems, technical and cryptographic information protection, taking into account the experience of the member states of NATO and the EU;

- creation of a cybersecurity training system for the security and defence sector agencies;

- development of international cooperation in the field of cybersecurity, intensification of collaboration between Ukraine and NATO, in particular within the framework of the NATO Trust Fund for enhancing Ukraine's cybersecurity capabilities.

The government of Ukraine was consistent and in early 2016 the Strategy on Cybersecurity of Ukraine was approved,[14] which defined a set of measures, priorities and directions for ensuring the cybersecurity of the state. The creation and operational adaptation of the state policy and achievement of compatibility with the relevant standards of the EU and NATO and the deepening of cooperation with them were foreseen. The document reveals the same approaches as the EU Cybersecurity Strategy, in particular the principles of "openness, accessibility, stability and security of cyberspace". In the military dimension of cybersecurity in Ukraine, NATO's approaches are used, in particular, cyberspace is also recognized as a domain of operations.

[13] https://zakon.rada.gov.ua/laws/show/287/2015

[14] https://zakon.rada.gov.ua/laws/show/96/2016/ed20180509

The law "On the Basic Principles of Cybersecurity of Ukraine",[15] approved in October 2017, contains terminology, taking into account the terminology of the EU and NATO, which allows clear distinction between types and objects of activity and fixes the areas of responsibility of participants in this field. For example, the law reflects such European principles as openness, accessibility, stability and security of cyberspace, as well as the need for interaction with the private sector and civil society in the field of cybersecurity.

The Law of Ukraine "On National Security", which came into force on June 21, 2018, in the Article 19 imposes the provision of cybersecurity on the Security Service of Ukraine.[16] Article 22 of the same Law admits the special role of the State Service for Special Communications and Information Protection of Ukraine (Derzhspetszviazok): "The State Service for Special Communications and Information Protection of Ukraine is a state body designated to ensure the functioning and development of the state system of government communications, National system of confidential communication, formation and implementation of state policy in the areas of cyber defence of critical information infrastructure, state information resources and information, whose protection is required by law, cryptographic and technical protection of information, telecommunications, use of the radio frequency resource of Ukraine, special-purpose postal mail, Feldjäger government communication, and other tasks in accordance with the law". Article 31 of the Law is devoted to the Cybersecurity Strategy of Ukraine as a document of "long-term planning, which defines the priorities of Ukraine's national interests in the field of cybersecurity, available and potentially possible cyber threats to the vital interests of a person and a citizen, a society and a state in cyberspace", priority directions, conceptual approaches to formation and the implementation of state policy, improving the effectiveness of key actors in providing cybersecurity, as well as the needs of budget financing.

The law provides for a "Comprehensive Review of the Security and Defence Sector", which is conducted by the decision of the National Security and Defence Council of Ukraine and comes into force by the Decree of the President of Ukraine. The comprehensive review of the security and defence sector includes "the review of the status of cyber defence of state information resources and critical information infrastructure", among others. The Cabinet of Ministers of Ukraine determines the procedure for conducting a special review of the Derzhspetszviazok, the status of cyber defence of critical information infrastructure, state information resources and information, the requirement for protection of which is established by law.

[15] https://zakon.rada.gov.ua/laws/show/2163-19

[16] https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2469-VIII

The Military Doctrine of Ukraine, approved on September 24, 2015, actually ignores the issues of cyber defence. Only the cyber defence of critical infrastructure is mentioned as a part of the competence of the Derzhspetszviazok: "ensuring the functioning of the Government communications of the Supreme Commander-in-Chief of the Armed Forces of Ukraine with officials of the Armed Forces of Ukraine, other military formations, law enforcement agencies of special purpose during their stay in the control points, providing cybersecurity of critical infrastructure objects".[17]

According to the mentioned documents, the basis of the cybersecurity national system is the SSU, the Derzhspetszviazok, the Ministry of Defence and the General Staff of the Ukrainian Armed Forces, the National Police, the National Bank of Ukraine, and intelligence agencies. The highest coordination body is the National Coordination Centre for Cyber Security as a working body of the NSDC of Ukraine. The main task of the Centre is to develop proposals to strengthen Ukraine's ability to combat military cyber threats, cyber-espionage, cyberterrorism, cybercrime and to provide cyber defence of information resources and critical infrastructure.

Long before the approval of the Cybersecurity Strategy of Ukraine, the Computer Emergency Response Team of Ukraine (CERT-UA) was created in 2007, which is a specialized division of the Derzhspetszviazok. It serves as the technical coordinator of state bodies, local self-government bodies, military formations, enterprises, institutions and organizations, regardless of ownership, on the prevention, detection and elimination of the effects of cyber incidents. CERT-UA acts on the same principles as the CERT-EU. This team also has the functions of operational interaction with foreign partners and international organizations for responding to cyber incidents, in particular as a part of the Forum of Incident Response and Security Teams (FIRST). Although at this Forum, Ukraine is represented by only one team, namely CERT-UA, while Poland is represented by 5 teams, Germany – by 31 teams, and the United States - by 90 teams.

The Security Service of Ukraine operates the Situation Centre for Cyber Security, which is aimed at identifying, preventing and neutralizing cybernetic actions against Ukraine. The National Police of Ukraine operates the National Contact Centre in a 24/7 format for the response and exchange of information on computer crimes.

Ukraine is at the forefront of countering cyber threats, and its experience is appreciated in the world. So, at the meeting on the situation in the Middle East on February 21, 2019, in Warsaw, the Minister of Foreign Affairs of Ukraine Pavlo Klimkin was asked to speak on cybersecurity. "*Our experience is very much*

[17] https://zakon.rada.gov.ua/laws/show/555/2015

appreciated, because, in addition to the usual discussions and speeches, I was asked to speak specifically on cybersecurity and information warfare. It is our experience that is used to a large extent now, "said Klimkin before this event.[18]

Thus, Ukraine has adopted and continues applying European and international standards in the field of cybersecurity; it has created and develops relevant bodies that can effectively interact with relevant EU and NATO bodies. However, because the law on the protection of critical infrastructure in Ukraine is still not adopted, Ukraine lacks a clear definition of critical cyber infrastructure that complicates the work of public authorities in this field and the application of common standards. Meanwhile, the experience of Ukraine allows it to be not only the recipient of assistance from the EU and NATO, but also a source of new knowledge, skills and methods of counteracting modern cyber threats.

[18] https://www.ukrinform.ua/rubric-polytics/2640332-klimkin-govoritime-pro-kiberbezpeku-na-blizkoshidnij-konferencii-u-varsavi.html

II. Cooperation of Ukraine with the EU and NATO for cybersecurity

The goals of the security **cooperation between the EU and NATO** coincide, and this is based not only on the fact that 22 countries are members of both the EU and NATO, but also on the desire to reciprocally fill the existing gaps in the security capabilities of each other, in particular in the field of cybersecurity. For the development of such cooperation, as well as interaction with other participants, namely, Ukraine, the Framework Document for a Joint EU Diplomatic Response to Malicious Cyber Activities was developed.

An important milestone in the development of cooperation between the EU and NATO on cybersecurity was the establishment of the links between the European Defence Agency and the NATO Cooperative Cyber Defence Centre of Excellence in 2013 for the exchange of information, joint exercises and activities, and avoiding duplication of research in the cyber sphere. The two structures conducted a series of joint exercises, including the already mentioned Cyber Coalition and Cyber Europe training, which became the platform for common approaches.

The current actualization of hybrid challenges and threats associated with Russia's aggression against Ukraine gives an additional impetus to deepening the interaction between the two organizations. In February 2016, before the approval of the Joint Declaration on EU-NATO Cooperation, the two organizations signed a Technical Cooperation Arrangement on Cyber Defence in areas of information exchange, training, research and exercises. As a result, practical cooperation is developed between the Computer Emergency Response Team (CERT-EU) and the NATO Computer Incident Response Capability (NCIRC), which became the signatories of the aforementioned technical agreement on behalf of the EU and NATO.

The new EU-NATO cooperation marked its second year at NATO Summit on July 11-12, 2018, in its new headquarters in Brussels. Collaboration between the EU and NATO has increased in all areas, from hybrid threats and cybersecurity to maritime cooperation. Cybersecurity is always present in their official documents.

As a part of the enhanced cooperation between the EU and NATO with the involvement of third parties, in particular on cybersecurity, there are currently three pilot countries: Moldova, Tunisia and Bosnia and Herzegovina. The third progress report on its implementation, endorsed by the EU and NATO Councils,[19] states that information sharing, including staff-to-staff political consultations, will be also available for Ukraine.

[19] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf

Photo 1. A Technical Arrangement signing between the EU and NATO, Feb. 10, 2016
(the signatories – the Head of CERT-EU, Freddy Dezeure, and the Chief of Cybersecurity at NCIRC, Ian West)
Source - https://www.nato.int/docu/review/2016/also-in-2016/cyber-defense-nato-security-role/en/index.htm

Ukraine has got a lot of skilled experts in the cyber sphere. However, they still lack interagency coordination and cooperation with international partners. For example, the EU Consultative Mission in Ukraine interacts with the Cyber police of Ukraine, the Security Service of Ukraine and the National Centre for Coordination of Cybersecurity under the NSDCU. Meanwhile, proper coordination remains an important issue, since it does not depend on the strategies or policies that they are developing. Similarly, the costs and efforts of donors depend on the level of inter-agency coordination in Ukraine.

Ukraine's cooperation with the EU and NATO in the field of cybersecurity is so far separate, although in some cases, mainly at the level of practical assistance, the two organizations carry out at least the coordination of their efforts, since this bilateral assistance should be coordinated in accordance with the principles of EU-NATO cooperation on cybersecurity.

The European External Action Service believes that the complex nature of cyberspace requires joint efforts by governments, the private sector, the expert community, the technical community, users and academics to counter current cyber threats. According to Elois Divol, a policy officer of the Cyber Policy Coordination, Conflict Prevention & Security Policy department of the European External Action Service, who participated in the International Conference "New Forms of NATO-EU Cooperation with Ukraine" on May 30-31, 2018 in Kyiv,[20] the EU draws attention to the need for adaptation of partner countries, including Ukraine, to the rules of

[20] https://geostrategy.org.ua/ua/component/k2/item/1473-post-reliz-novi-formati-spivpratsi-nato-i-es-z-ukrayinoyu

cybersecurity of the EU, priority among which is the certification of software, the process of reporting, the introduction of standards of responsibility for actions in cyberspace.

At the multilateral level, the EU is guided mainly by the goals set out in the Joint Staff Working Document on "Eastern Partnership – 20 deliverables for 2020: focusing on key priorities and tangible results", where in the Security section three out of ten groups of tasks relate to cybersecurity, in particular, on the creation of full-fledged operating units for combating cybercrime, the development of public-private cooperation and international cooperation in the field of cybersecurity. Ukraine has either already fulfilled these tasks, or has all real chances to accomplish by 2020.[21] Ukraine approved the Cybersecurity Strategy of Ukraine, implements the Criminal Cybercrime Convention and Directive 2008/114 / EC on the protection of critical infrastructure, has created the necessary institutions that interact with the EU and non-state institutions (for example, CYS-Centrum and Ukrainian Cyber Forces).

At the EU-Ukraine bilateral level, cybersecurity is at the centre of attention. So, during the fifth meeting of the Association Council on December 17, 2018 in Brussels, both sides emphasized the need for further cooperation in combating cyber and hybrid threats in the interests of the safety of their citizens. In this regard, the Association Council welcomed the EU commitment to continue supporting Ukraine in the field of cybersecurity.[22]

In 2017-2018, the EU implemented a number of activities under the TAIEX technical assistance instrument in three areas: creation of an appropriate legislative framework in Ukraine; creation of public-private partnership and promotion of organizational aspects of national cybersecurity structures; support of technical abilities and skills in state authorities responsible for cybersecurity.

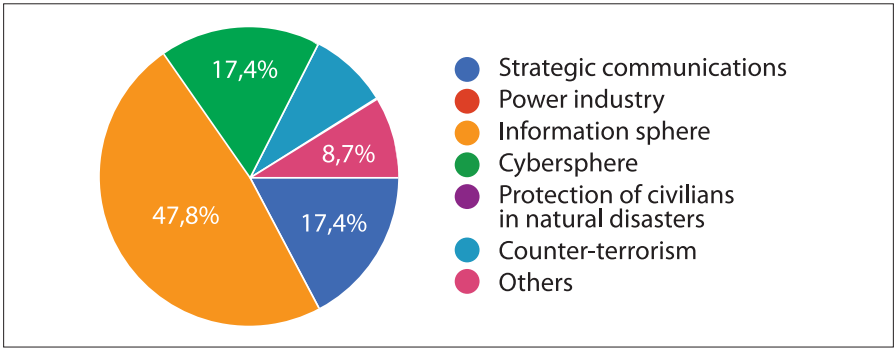
The EU assists Ukraine through its EU Advisory Mission to Ukraine (EUAM), which, among other things, provides assistance in the area of countering cyber threats across whole Ukraine. More than 2.5 million euros were allocated by the EUAM to various projects helping Ukraine in the area of cybersecurity. The mission promotes the improvement of technical equipment of Ukrainian law enforcement agencies, conducts trainings, exchanges of experience and panel discussions. The events involve experts from Europol and other EU institutions.

Cyber field is a priority in the development of cooperation between Ukraine and NATO. In particular, Ukrainian experts, who participated in the international

[21] http://eap-csf.org.ua/wp-content/uploads/2017/10/Report_Ukrainian.pdf

[22] https://eu-ua.org/novyny/spilna-zayava-dlya-presy-za-rezultatamy-5-go-zasidannya-rady-asociaciyi-mizh-ukrayinoyu-ta?fbclid=IwAR3m9I-dcxFVi18jxynTEpsuTk0BiZTBoSCzf-NSmFygQcc_6gEJxAM5D1Y

round table "Ukraine-NATO: Non-military Cooperation as Response to Common Hybrid Threats" organized by the Centre for Global Studies "Strategy XXI" and the Konrad Adenauer Stiftung Office in Ukraine on February 9, 2017 in Kyiv, put cybersecurity in the second place among the priority directions of joint NATO-Ukraine counteraction to hybrid threats.[23]



Pic. 2. Key areas of Ukraine-NATO common countering to hybrid threats.

The cyber cooperation between Ukraine and NATO has been established that is registered every year in the Annual National Programs under the auspices of the NATO-Ukraine Commission (ANP) in a separate section on Cyber Security.[24] The purpose of this cooperation is "to improve the national system of cybersecurity as a component of the information security system, its legal conceptual framework and practical mechanisms for counteracting the Russian aggression in cyberspace". According to the ANP, Ukraine strengthens the cooperation of state, including law enforcement and special bodies, with a private IT sector that corresponds to the EU and NATO approaches to counteracting cyber threats.

The Trust Fund for Cyber Defence launched in 2014 and the Comprehensive Assistance Package endorsed in 2016, where cybersecurity is identified as a priority, contribute the NATO-Ukraine partnership. The goal of the Trust Fund led by Romania is to ensure the development of its own anti-cyber threats groups and Computer Security Incident Response team capacity (CSIRT1) in Ukraine, including laboratories for investigating cyber incidents. NATO is helping Ukraine to improve its legislation, develop strategies and policies, provide practical support to the development of technical infrastructure, and prepare and develop the capacity of the cyber defence, which will remain a priority in the near future.

[23] https://www.kas.de/veranstaltungen/detail/-/content/ukraine-nato-nichtmilitaerische-zusammenarbeit-als-gemeinsame-antwort-auf-hybride-bedrohungen

[24] https://www.president.gov.ua/documents/892018-23882

In 2014, a project was launched to create situational centres for responding to computer incidents for monitoring cybersecurity events, as well as laboratories for investigating incidents in cyber space and eliminating their consequences. In June 2017, Ukrainian institutions successfully received the appropriate equipment, and in July 2017 the first stage of the Trust Fund was completed, the main beneficiaries of which were the SSU and the Derzhspetszviazok. In January 2018 the Situational Centre for providing cybersecurity of the SSU was opened. NATO has allocated more than 1 million USD for this project. Other Ukrainian ministries, including the Ministry of Foreign Affairs of Ukraine, also receive equipment and software from NATO needed for the protection of information infrastructure.

As part of the training of Ukrainian experts, in 2015, Estonia, as a member of the Trust Fund, organized a five-course training on incident response in cybersecurity, strategic level training (cyber policy and cyber strategy) and the operational level training on cybersecurity. Located in the capital of Estonia, the NATO Cooperative Cyber Defence Centre of Excellence explores the situation in Ukraine and collaborates with Ukrainian actors responsible for this issue.

Ukraine is one of the partner countries participating in the Defence Education Enhancement Programme (DEEP) of the NATO Cybersecurity Training Program. So, in September 2018, such a course was conducted on the basis of the Zhytomyr Military Institute named after Serhiy Koroliov. The exercise involved cyber operations, both defensive and offensive ones, in support of an overarching military mission scenario.[25]

Every year, Ukrainian military experts in the field of cyber defence take part in the large-scale NATO Multinational Training, called "CWIX" (Coalition Warrior Interoperability Exercise) held at the training centre in Bydgoszcz, Poland. In 2019, this year three-week training sessions are scheduled for May-July 2019.

In the future, in the sphere of cybersecurity, NATO will focus on developing Ukraine's capabilities, providing the necessary equipment and training, which should enable Ukraine to protect its infrastructure against cyber attacks. At the same time, the opposition and the cessation of activities of persons residing in the territory of NATO and the EU member states and provide various support to terrorist and extremist activities, in particular, activities of the so-called "DNR" and "LNR", and citizens of Russia and other countries that are involved in aggression against Ukraine will remain as a very important issue.

In the future, the development of cooperation between the EU and NATO in the field of cybersecurity Ukraine may be in the spotlight if the Ukrainian government will support the pace of reforms and improve the level of inter-agency coordination.

[25] https://www.nato.int/cps/en/natohq/news_159840.htm?selectedLocale=en

III. New cyber challenges and threats

Russian activities in cyberspace are a major challenge for Ukraine in the field of cybersecurity. Russia uses cyberspace as a space for new opportunities to carry out not only intelligence activities against Ukraine, but also to perform special operations for the covert penetration into cybersecurity networks of public authorities and the establishment of remote control over critical infrastructure objects in order to obtain benefits and secure their interests in information, military-political, financial-economic, and energy spheres.

The American company FireEye, specializing in international cybersecurity issues, identified a group of hackers from a number of groups of Advanced Persistent Threats, which for a long time conducted information operations under orders of the Russian Government. It received the code name ART 28 (also known as Fancy Bear, Pawnstorm, CyberCaliphate, Cyber Berkut, Tsar Team, etc.), it is identified as a cyber unit of the General Staff of the Russian Armed Forces. Since 2007, the specific feature of ART 28 was the specialization in obtaining information on defence, military-political and geopolitical subjects. The objects of attacks were computer networks of a number of state institutions and organizations from Central and Eastern Europe, in particular Poland, the Czech Republic, Ukraine, Georgia, as well as NATO and the OSCE.

Since 2014, Ukraine has been used as a testing ground for new cyberattacks by Russian special services and groups of hackers controlled by them. There were recorded several types of attacks aimed at informational and psychological impact on the population, illegal gathering of information, shutdown of activities of central authorities, and also causing material damage to the state and citizens due to the disruption of information and telecommunication systems on critical infrastructure objects.

Reference. *The presence of a serious potential for cyber-attacks in Russia was demonstrated in the course of the known attack on Estonia in 2007. An indication of the direction for further build-up of cyber-capacities was 2012. On October 17, 2012, the Ministry of Defence of the Russian Federation together with the Agency of Strategic Initiatives, the Ministry of Education and Science of the Russian Federation and the Moscow Higher Technical School named after Bauman announced the All-Russian competition for research works, one of the topics of which was Methods and Means of Circumventing antivirus systems, network security tools, protection of operating systems.*[26] *Based on*

[26] Russian competition for research works and ideas for strengthening country's defense capabilities. 13.10.2012. http://inno.nsu.ru/news/2012-10-13.htm

> *the title of the topic, Russian specialists evaluated this as a selection of projects and personnel for the development of combat offensive viruses in order to overcome the protective systems of a probable opponent.*[27] *According to Russian experts, "this kind of questioning is fundamentally divergent from a purely defensive strategy in the field of information confrontation, which was prescribed in the Military Doctrine of the Russian Federation 2010, as well as in the foreign policy initiatives of Russia.*[28]

A sharp shift in 2013 in the direction of increasing activity in cyberspace can be noted after President of the Russian Federation Vladimir Putin signed the adopted Law No. 31c dated January 15, 2013, according to which the FSB of the Russian Federation became responsible for creating a system of cyber defence and counteracting cyber-attacks against Russian critical infrastructure. Soon, on February 13, under the auspices of the military department, an informational warfare unit in the General Staff of the Armed Forces of the Russian Federation was announced. Only 4 years later, on February 22, 2017, at a special meeting in the State Duma, the Minister of Defence of the Russian Federation S. Shoigu recognized the creation of information operations forces. The Chief of the General Staff of the Armed Forces of the Russian Federation in 2004-2008 Army General Yuriy Baluyevsky, commenting on the statement of S. Shoigu, said that victory in the information warfare was often more important than in the classical war: *"Victory over the enemy in this war can be much more important than victory in the classical military confrontation, since it is bloodless, and the effect is spectacular – it depletes and paralyzes all the authorities of the enemy state."*[29] Despite the activity of the Russian Ministry of Defence in the cyber sphere, the FSB, FSO and FSTEC have similar opportunities.

The confession of S. Shoigu in 2017 is a confirmation that Russia was purposefully preparing for aggressive actions not only in traditional warfare, in the information propagandistic dimension, but also in cyberspace. This coincides with the beginning of the hybrid-type aggression against Ukraine, and now it can be stated that with the cyber-penetration in the US, the EU and NATO countries, which began to acquire revealed forms during the presidential election campaign in 2016 in the United States. The main cyber forces of Russia are concentrated on the United States. Europe is not neglected, but here the main front is the informational and propagandistic. However, as election campaigns are held in a number of Western European countries in 2017-2019, the Russian cyber offense to Europe is intensifying.

---

[27] Ministry of Defense announced a tender for offensive warfare. Vzglyad. 18 October 2012. http://vz.ru/news/2012/10/18/603077.html

[28] Oleh Demydov. "US Cyber Command: Lessons for Russia". "Security Index", Y2013, Num. 3 (106), Volume 193 http://www.perspektivy.info/rus/konturi/kiberkomandovanije_ssha_uroki_dla_rossii_2013-11-15.htm

[29] Nikita Buranov. Fundamentally New Troops. «Expert Online». http://expert.ru/2017/03/1/kibervojna/

As for the Ukrainian cyber battlefield of the Russian hybrid aggression, in 2014 the Cyber Berkut group (ART 28) assumed responsibility for attacks on sites of state bodies and public organizations of Ukraine and a number of western countries. The first attacks were carried out in March 2014 during the occupation of Crimea when a number of Ukrainian web resources were temporarily blocked and an attack on the three Internet resources of NATO was announced. Significant actions of Cyber Berkut in the informational and cyber space are:

- creating obstacles in the work of the CEC of Ukraine on the eve of the presidential elections of Ukraine on May 23, 2014;

- blocking the work of the sites of the Ministry of Internal Affairs of Ukraine and the General Prosecutor Office of Ukraine dated April 4, 2014;

- DDoS attacks on the website of the Cabinet of Ministers of Ukraine on April 10 and April 14, 2014;

- blocking of cellular telephones belonging to members of the Government of Ukraine;

- blocking of leading news portals of UNIAN and LIGABusinessInform;

- blocking the site of the President of Ukraine P. Poroshenko on July 29, 2014.

Thus, these actions are synchronized in time with the diffuse phase of the Russian invasion into Ukraine in Donbas. Thus, the cyber front against Ukraine was opened simultaneously with the military component of the hybrid aggression of Russia.

In February 2015, with the support of Russian law enforcement agencies, an identical hacking organization called SPRUT (the so-called "System of counteraction to Ukrainian terrorism") was created. This organization attacks official sites of the governing bodies of regional administrations, the Ministry of Defence of Ukraine, the Security Service of Ukraine, the General Staff of the Armed Forces of Ukraine, the Main Directorate of Intelligence of the Ministry of Defence of Ukraine.

At the end of 2015, in order to increase the effectiveness of the information war against Ukraine, the executive management of the General Staff of the Armed Forces of the Russian Federation created a Centre for Information Warfare (CIW) in Novocherkassk as part of the Centre for Territorial Forces of the Southern Military District of the Russian Federation. A powerful software and hardware complex were delivered to Donetsk to distribute cyber attacks (DDoS-attacks).

On December 29, 2016, for the first time officially and publicly, in a Joint Statement of the US Department of Homeland Security, the Office of National Intelligence and the Federal Bureau of Investigation, Russia was accused of hacking attacks on

the United States.[30] The activity of the Russian Federation are reflected in the Joint Analysis Report of the Department of Homeland Security and the FBI. It is noted that within ten years, Russian intelligence services have conducted cyber-operations targeting the US government organizations, critical infrastructure, think tanks, universities, political organizations, and corporations.

Thus, it took almost a decade for the United States and Europe to come to an official conclusion about Russia's unfriendly actions in the cyberspace against the West. Such lethargy and slowness only play on the Russian script of cybernetic *Pearl Harbour*. Russia is working to create a state of disinformation, chaos, and disorganization of the public administration system in D-Day, ideally to manage strategic nuclear forces in the United States, and to get a window of opportunity for nuclear blackmailing the West.

In 2013-2017, cyber assaults against Ukraine were carried out with the use of ART attacks (Snake, Uroboros, Sofacy / APT28, Epic Turla, Black Energy 2 and 3, Armageddon and others), which are typical for Ukraine.[31] In June 2017, Ukraine suffered a major attack by Petya-A computer virus. The virus-encryptor has penetrated a number of networks of Ukrainian public and private institutions, in particular, the site of the Cabinet of Ministers and a number of ministries, the Pension Fund, Kyiv municipality, a number of banks, large public and private enterprises.[32] Cyber Police of Ukraine managed to stop the next wave of cyber-attacks and establish that it was preceded by a collection of data on Ukrainian enterprises. According to experts, this information was the true purpose of this cyberattack for further cyber intelligence and subversive actions.[33] Due to preventive measures, in October 2017 Ukrainian law enforcement officers managed to avoid losses and mass spread of cyber-attacks to certain objects, in particular, Odesa airport, Kyiv subway, Ministry of Infrastructure.[34]

Another threat in the context of Russian aggression is the work of hired Chinese cyber groups in favour of Russia. Some Ukrainian experts concluded that Russian

---

[30] «Joint DHS, ODNI, FBI Statement on Russian Malicious Cyber Activity». https://www.dhs.gov/news/2016/12/29/joint-dhs-odni-fbi-statement-russian-malicious-cyber-activity

[31] Analytical Report on the Annual Message of the President of Ukraine to the Verkhovna Rada On the Internal and External Situation of Ukraine in 2016. – K. : NISS, 2016. – 688 p.

[32] The SSU has established the RF special services involvement in the Petya –A virus attack, 01.07.2017. https://www.ukrinform.ua/rubric-technology/2257453-sbu-vstanovila-pricetnist-specsluzb-rf-do-ataki-virusu-petyaa.html

[33] The SSU warns of possible cyber-attacks on institutions and enterprises, 18.08.2017. https://www.ukrinform.ua/rubric-society/2288607-sbu-poperedzae-pro-mozlivu-kiberataku-na-merezi-ukrainskih-ustanov-ta-pidpriemstv.html

[34] The minister of Infrastructure commented on the consequences of the cyber attack, 25.10.2017. https://www.ukrinform.ua/rubric-technology/2331042-ministr-infrastrukturi-prokomentuvav-naslidki-kiberataki.html

cyber groups are carrying out their operations using the technical capabilities of Chinese hacker organizations.[35] This became possible after the international legal validation of the joint Russian-Chinese activity in cyber space. An agreement on cooperation in the field of international information security was signed between Russia and the PRC at the intergovernmental level in 2015. The agreement is a legal framework for cooperation between Russian and Chinese cyber groups, which are supported at the state level in both countries and are the units of the respective intelligence organizations of both countries. Thus, by attracting Chinese outsourcing, the Russian Federation is capable of concentrating powerful cyber resources for cyber warfare.

The saturation of the Ukrainian market with Chinese mobile communication equipment with the corresponding software also arouses concern. Against the backdrop of resonant investigations in Europe and the United States regarding the hidden possibilities of Chinese products for information gathering, it is important for Ukraine to cooperate with NATO and the EU to prevent the possible negative consequences of their massive use and prevent the emergence of such equipment and software in the system of state governance and military command.

An analysis of Russian sources indicates that, at the conceptual level, cyber weapons are determined more broadly than commonly accepted in the West. That is, it is not just a certain software product for interference with the work of computers and networks, but a complex of remote hidden effects on the machine or human-machine system, which leads to loss of its functionality or hidden reprogramming of its functions, which does not allow to fulfil the target task.[36] Examples could be: the failure of an on-board computer control system for the fire of a warship, the miss off the target of a missile, or its sudden self-destruction on an approach to the target, the spoofing of the GPS system, which leads to critical deviations in determining the coordinates of targets for fire, etc. A qualitatively different effect can be given by the complex application of electronic intelligence, electronic warfare and cyber weapons.

In Russia, prototypes of cyber weapons have been developed to neutralize the critical infrastructure of an enemy in order to increase the effectiveness of the subsequent first strike or to maximize the weakening of its ability to withstand. It is also specific that the action of this type of cyber weapon equates to a disarming nuclear strike. Moreover, such a cyber weapon cannot have any deterrent potential.

---

[35] International cooperation in the field of cybernetic security: State Priorities. R.V. Lukianchuk. Bulletin of the NAPA 04.2015. http://visnyk.academy.gov.ua/wp-content/uploads/2016/01/2015_4_8_ukr.pdf

[36] Problems in cyber weapon classification. V.V.Kabernik. Bulletin of MGIMO. №2, 2013. https://cyberleninka.ru/article/v/problemy-klassifikatsii-kiberoruzhiya

In his speech at the annual meeting of the Academy of Military Sciences on March 2, 2019, Valeriy Gerasimov, the Chief of the General Staff of the Armed Forces of the Russian Federation, pointed to a significant increase of the importance of the information sphere in the modern warfare: *"At the same time, information technologies constitute, in fact, one of the most promising weapons. The information sphere, without clearly defined national boundaries, provides the possibility of remote, covert influence on critical information infrastructure, as well as on the population of a country, directly affecting the condition of national security of the state. That is why the elaboration of the issues of preparation and conducting of information actions is an important task of the military science. Digital technology, robots, unmanned systems, electronic warfare - all this should be on the agenda for the development of the military science, including the military strategy".*[37] As we see, the emphasis is on the complex application of the latest means of conducting a modern war of hybrid type, but with a focus on critical information infrastructure. It is obvious that, according to the plan of the General Staff of the Armed Forces of the Russian Federation, this should lead to a dysfunction or at least a paralysis of the system of state and military control over an enemy, with its subsequent chaotization.

In the presidential and parliamentary elections in 2019 in Ukraine, as well as during the elections to the European Parliament, Russia would test the updated interference technology in the electoral process. Its special feature is to remove as much as possible the disguising signs of interference, by which Ukrainian and Western cyber experts identify a Russian actor. Most likely, for this purpose, the corresponding "nests" and networks have been created on the territory of Ukraine and the EU member states. In turn, the Ukrainian and European elections should become the next stage of cyber enhancement with a sight for the presidential elections in the USA in 2020.

[37] Army General Valeriy Gerasimov, Chief of the General Staff of the Armed Forces of the Russian Federation, spoke at the general meeting of the Academy of Military Sciences. 04.03.2019. http://redstar.ru/vektory-razvitiya-voennoj-strategii/?attempt=1

IV. Strengthening Ukraine's interaction with the EU and NATO in countering cyber threats

In the framework of further development of Ukraine's interaction with NATO and the EU, first of all, it is necessary to take into account the current trends of cooperation between the EU and NATO. Further EU-NATO-Ukraine cooperation in the field of cybersecurity should be focused on the following areas:

- to complete the establishment of a clear cybersecurity coordination working system for the full implementation of the Cybersecurity Strategy of Ukraine to involve all national actors, including non-governmental organizations, and make NATO, the EU and other organizations' assistance more targeted and effective;
- to use the experience and practice of the EU and NATO in order to create a broad national cybersecurity certification scheme, develop a plan to respond to large-scale incidents and crises, deepen public-private partnerships and strengthen research;
- to initiate the accession of Ukraine to the NATO Cooperative Cyber Defence Centre of Excellence, which will help Ukraine to implement best practices and deepen its cooperation with the Alliance in this area;
- to increase Ukraine's defence technical potential in cybersecurity with the assistance of the NATO Cybersecurity Trust Fund and in cooperation with Romania;
- to develop cooperation on strengthening cybersecurity in Ukraine in order to prevent and neutralize possible Russian interference during electoral campaigns in Ukraine;
- to continue identifying critical infrastructure and its key operational vulnerabilities;
- to work out a national Emergency Response Plan in cyber space;
- to develop an instrument of risk sharing through the use of secure cloud services in order to minimize possible losses in case of cyber attacks on the data bases of state authorities;
- to use the best Western experience in order to strengthen interagency cooperation and state-private partnership, as well as to develop a specific effective mechanism for its practical application;
- to propose NATO and the EU to attract more external expert assistance for Ukraine;
- to combine efforts to develop a system of motivation for professionals engaged in cybersecurity and cyber defence.

Along with the strengthening of the protection of Ukrainian cyberspace with the Alliance’s assistance, the important direction of Ukraine-NATO cooperation is to counteract and cease the activities of persons living in the territory of NATO member countries and providing various types of support for terrorist and extremist activities. It is also necessary to improve the level of cooperation between Ukraine and the EU member states in blocking work at all levels, especially at the level of private campaigns (e.g. PayPal), the activities of members of the so-called “DNR” and “LNR” and citizens of Russia and other countries that are involved in the aggression against Ukraine, especially those who are included into the sanction lists.

Another important area of cooperation could be monitoring of Russian and Chinese cyber-activities, the interaction of cyber-organizations of both countries. The common attention may be focused on studying Russia’s possibilities to use technological fibre-optic communication lines of trans-border gas pipeline systems such as North Stream 1, North Stream 2, Turkish Stream and their extensions across the EU and NATO territories to address non-core tasks, including cyber-espionage.

Conclusions

According to the decision of the Coordination Council of the NATO Trust Fund in 2017, the further direction of developing the national cybersecurity system was aimed at increasing the technical capabilities of Ukraine in the area of cybersecurity of critical infrastructure objects by equipping them with automatic sensors and connecting the Situation Centres of the Derzhspetszviazok and the SSU to the national network, as well as the creation of Cyber Security Centres in the system of the Armed Forces of Ukraine and the National Police with their further integration into the National Network of the Situation Centres.[38] This direction is strategically important for Ukraine in view of Russia's further possible actions against Ukraine, NATO and the EU that is quite predictable in the context of the latest military-strategic innovations of the General Staff of the Armed Forces of Russia.

In an interview to the BBC in June 2018, Former director of the US National Security Agency and 1st Commander of USCYBERCOM Keith Alexander stated: *"Obviously, after some time Ukraine, its energy and financial systems, and government structures are undergoing cyberattacks. Russia will try to represent Ukraine as a territory where the state exists only on paper and cannot function."*[39] After strong cyber attacks in Ukraine in 2015, 2016 and 2017, 2018 was the year of relative calm on the cyber frontline. This is probably due to the fact that Russian cyber structures, conducting «reconnaissance by an attack» to the Ukrainian information and communication networks, are preparing for a cyber-strike, which can be synchronized with the escalation of the Russian military actions against Ukraine, when the Putin regime decides that the West has been finally overloaded with its own problems and it has more important things than Ukraine to think about. The calm is also explained by the period of two electoral campaigns in Ukraine, when Russian propaganda and cyber efforts focus on producing chaotic situation in the country through provoking and fuelling conflicts between rival political forces on the principle of "war of all against all".

It is important for Ukraine, NATO and the EU to continue interacting in the cyber field. Against the backdrop of broadening and deepening multilateral cooperation between Ukraine and NATO, Ukraine and the EU, enhancing Ukraine's cybersecurity in the context of strengthening its overall resistance capacity in various spheres will mean the closure of another vulnerable zone of the European cyberspace and the emergence of an additional shield that will protect Europe from the East.

---

[38] Security Service of Ukraine has held a ceremony for the completion of the first phase of the NATO Trust Fund to assist Ukraine in strengthening cyber defence. 04.07.2017. https://www.ssu.gov.ua/ua/news/1/category/2/view/3668#.V3SsDFLC.dpbs

[39] Get ready, because Russia will launch a cyber-strike to Ukraine – an expert from the US. Georgiy Erman. BBC News Ukraine. June 4, 2018 https://www.bbc.com/ukrainian/features-russian-44353054

Ukraine – EU – NATO Cooperation
for Countering Hybrid Threats in the Cyber Sphere

Prepared on the results of the research of the Centre for Global Studies "Strategy XXI" on countering the hybrid aggression of the Russian Federation and strengthening Ukraine's cooperation with the EU and NATO.

With the financial support of the Konrad Adenauer Stiftung Office in Ukraine.

The separate opinions expressed in the analytical paper are the point of view of experts of the Centre for Global Studies "Strategy XXI" and do not necessarily reflect the vision of the Konrad Adenauer Stiftung.

© Centre for Global Studies "Strategy XXI"

Reference to the publication, authors and the website http://geostrategy.org.ua are required.

Kyiv
2019

Ukraine – EU – NATO Cooperation for Countering Hybrid Threats in the Cyber Sphere

© Centre for Global Studies «Strategy XXI»