УДК 351.862.4(342)ЄС:342.232.5

THE EUROPEAN EXPERIENCE OF PUBLIC-PRIVATE PARTNERSHIP IN THE SHPHERE OF CYBERSECURITY: OPPORTUNITIES FOR UKRAINE

ЄВРОПЕЙСЬКИЙ ДОСВІД ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ КІБЕРБЕЗПЕКИ: МОЖЛИВОСТІ ДЛЯ УКРАЇНИ

Matviyenko V.M.
Doctor of Historical Sciences, Professor, Head of the department of International Organizations and Diplomatic Service of the Educational and Scientific Institute of International Relations of Taras Shevchenko National University of Kyiv. E-mail: vikmaryuniv@ukr.net

Petushkova H.E.
Ph. D. student at the department of International Organizations and Diplomatic Service of the Educational and Scientific Institute of International Relations of Taras Shevchenko National University of Kyiv. E-mail: annpetushkova1@gmail.com

Матвієнко В.М.
Доктор історичних наук, професор, завідувач кафедри міжнародних організацій і дипломатичної служби Навчально-наукового інституту міжнародних відносин Київського національного університету імені Тараса Шевченка. E-mail: vikmaryuniv@ukr.net

Петушкова Г.Е.
аспірант Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка
E-mail: annpetushkova1@gmail.com

Abstract. *The article examines the process of initiation and development of Public-Private Partnership (PPP) in the EU, including the Great Britain, in the field of cyber security. The main stages of the formation of the PPP are considered, the key factors contributing to the intensification of cooperation in this direction are analyzed, as well as challenges that arise during the development of the partnership.*

The description of the current state of the cyberspace of Ukraine is given, taking into account the problems of the development of PPP. The main advantages and disadvantages of the existing system are described and recommendations, which are likely options for the future development of PPP in the field of cyber security, are offered.

The opinion about the necessity of a thorough study of the problem of PPP development in the field of cyber security in Ukraine is advocated, taking into account the European experience according to a scientific and political-strategic context.

Key words: *public-private partnership, Europe, cyber security, Ukraine, models of cyber security partnership development, critical infrastructure objects.*

Анотація. *У статті досліджується процес започаткування та розвиток державно-приватного партнерства (ДПП) в ЄС, включно з Великобританією, у сфері кібербезпеки. Розглядаються головні етапи становлення ДПП, аналізуються ключові чинники, що сприяють інтенсифікації співробітництва за даним напрямком, а також виклики, які виникають при розбудові партнерства.*

Дається характеристика поточного стану кіберпростору України, з урахуванням проблематики становлення ДПП. Описуються основні недоліки і переваги наявної системи та пропонуються рекомендації, які є вірогідними варіантами майбутнього розвитку ДПП у сфері кібербезпеки.

Обстоюється думка про необхідність ґрунтовного дослідження проблеми розбудови ДПП у сфері кібербезпеки в Україні, з урахування європейського досвіду, у науковому та політико-стратегічному контексті.

Ключові слова. *державно-приватне партнерство, Європа, кібербезпека, Україна, моделі розвитку партнерства з кібербезпеки, об'єкти критичної інфраструктури.*

Problem statement. The mainstreaming of the issues of the study of the process of building the European Public-Private Partnership (PPP) in the field of cyber security can be explained by the significant increase of malicious cyber activities of other countries in Ukrainian area. It can be stated that in recent years, especially before the beginning and during the full-scale war of the Russian Federation against Ukraine, the problems of building a cyber security PPP (Cyber PPP – CPPP) have sharply come up. An important condition for increasing the stability and development of the cyber potential of the state is to ensure partnership with the private sector due to the creation of a legal basis for cooperation, a clear separation of powers of cyberspace subjects and the establishment of effective communication. In turn, the experience of developing the CPPP of European countries is unique that makes a necessity of a scientific analysis of various forms of interaction.

The purpose of the article is to determine problem issues and perspectives of forming the CPPP in Ukraine according to a study of the peculiarities of the European experience about creating the CPPP and consideration of the current state of the cyberspace of Ukraine. Trying to achieve this goal, the author sets himself the following tasks:

- to investigate the development of PPP in the field of cyber security in the European area;
- to describe the main problems of forming CPPP in Ukraine;
- to define a possible situation that can contribute to further progress in establishing a partnership between country and private sector in sphere of cyber security.

The analysis of recent research and publications. The issue of CPPP is under active consideration by a wide range of foreign and domestic scientists, including the agencies responsible for the implementation of the cyber security strategy. Among foreign researchers, their own interpretations of the CPPP are given by M. Carr, J. Grimmelmann, A. Jagasia, M. Kostiainen, V. Kouwenhoven, T. Moore. L. Clinton defends the thesis about the importance of coordinating the role of partners, responsibility and effective management of relationships to cover all areas of cyber security [*Clinton, 2011: 98*]. The key EU subject in sphere of CPPP is European Union Agency for Network and Information Security, ENISA is actively investigating the models and practice of PPP. During the research, we will be guided by the thorough studies of ENISA: Good Practice Guide on Cooperative Models for Effective PPPs and Public Private Partnerships (PPP) - Cooperative models, that reveal the problem issues of setting up CPPP in Europe. In turn, the formation of the general research position was influenced by works of scientists such as D. Dubov, A. Paziuk, V. Boyko, S. Hnatyuk, T. Isakova, M. Ozhevan, A. Pokrovska, O. Frolova, O Kuchmiy. NISS scientists have researched the problem of CPPP in detail, with an emphasis on the organizational and legal component of partnership in Ukraine. The views of many researchers reach a consensus on the need of the implementation of the CPPP in order to increase the level of stability of national security. S. Goldsmith, W. D. Eggers, note the importance of analyzing the problem of the form in which the CPPP should be implemented, and not whether the state needs a PPP in the sphere of cyber security in general.

Presentation of the main research outcomes. The innovation and dynamism of the development of cyberspace requires the deepening of cooperation and cooperation between subjects in order to increase the stability of a cyber security system, which is one of the "pillars" of international stability. According to the increase of the number of interactions and partnerships between elements - the state, the private sector, the scientific community, etc. – further institutionalization of relations, legal regulation and the creation of a certain PPP model are considered necessary. ENISA provides the following definition: «public – private partnership (PPP) is a long – term agreement/ cooperation/ collaboration between two or more public and private

sectors and has developed through history in many areas» [*ENISA, 2017: 7*]. Public-private partnership in the sphere of cyber security is an effective form of establishing cooperation between representatives of the public sector and private structures. It is worth noting that PPP is not only public-private cooperation, it also includes a clear system and established communication between public-public and private-private sectors.

European national cyber security strategies have a common element - cooperation at all levels, but due to the different understanding of culture and different political systems, there is no universal model for creating a CPPP, thus, in reality, any European model cannot work in another country. Due to the existing practical experience of European countries, it is possible to highlight certain challenges that all models face:

- a total absence of hierarchy of governance and legal framework, as well as dialogue and effective communication;
- lack of financial support from the state budget and other state resources, that does not correlate with the capabilities and expectations of the private sector;
- low level of popularization of CPPP among Small and Medium Enterprises (SME);

Acquis communautaire in the sphere of cyber security and arising the CPPP models in Europe started developing rapidly in recent years, what is proved by the level of cyber incidents in relation to European companies. The political context of the European Union includes several directives and strategies that have elements of cooperation in the field of digital technologies and cyber security. The Digital Single Market Strategy (DSM) 2015 reveals the role of the digital economy, which is closely related to the interaction of the private sector and the state. The goal is to create a favorable investment climate for digital networks, to develop investor confidence, and to establish conditions for the mobilization of private investments [*A Digital Single Market Strategy for Europe, 2015: 17*]. In the spring of 2022, political agreement was reached on a package of two regulatory acts: 25 March – Digital Markets Act, 23 April – Digital Services Act, the adoption of the text by the Council of the European Union expected [13]. This legislative package has two goals - to create a safer digital area and equal conditions for the development of innovation and competitiveness. The scope of the law included a large category of online services, from basic websites to internet infrastructure services and online platforms. The creation of an independent body which purpose will be to ensure the consistent application of the legislative package of DMA and DSA according to the principle of functioning of the European Data Protection Board is under consideration.

In 2013, the European Commission presented the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace [*Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, 2013*]. This strategy indicates the importance of achieving cyber persistence as a strategic priority, and that effective cooperation between public authorities and the private sector is an important element of its provision.

Directive (EU) 2016/1148 – NIS Directive of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [*Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*] forms the first practical aspects of cooperation, in contrast to previous documents, for the development of the PPP structure in the field of cyber security in the European space. We can talk about increasing the level of awareness among operators of basic services, citizens, that is more easily achieved within the framework of PPP and that forms a general level of understanding. NIS Directive obliged states to identify service operators in certain sectors, which is also easier to implement through cooperation with the private-industrial sector, a especial importance has the issue of critical infrastructure protection. The implementation of the NIS Directive is not only about adjusting the legislation, but also about providing recommendations to the industry, including digital service providers, thus, there is an element of cooperation between public and private actors. In July 2016, the European Commission published a Communication on strengthening the European cyber resilience system and developing a competitive, innovative cyber security industry [*COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN*

PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry], that opened the way to the creation of a contractual public-private partnership platform – the European Cyber Security Organization (ECSO). ECSO unites representatives of national public administrations and the private sector and has to develop the PPP ecosystem in Europe through the forms of consultations and rational distribution of investments in research, innovation, which is co-financed through funds of the Horizon program. In accordance with the transformation of the threat from new ICT technologies, on May 13, 2022, a political consensus was reached on the text of the future document «the NIS2 Directive: A high common level of cybersecurity in the EU», which sets new goals for increasing the level of cyber persistence by introducing rules that ensure that all public and private organizations that implement important functions for the economy and society in the internal market are obliged to take appropriate cyber security measures. This is planned through the fixation of further coordination of 1) security requirements and incident reporting; 2) provisions that regulate national supervision and law enforcement; and 3) capabilities of relevant state structures [14].

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [*Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA*] has strengthened the powers of ENISA, giving the agency a key role in the cybersecurity certification system, as well as expanded operational cooperation and coordination in case of cross-border cyberattacks. Some provisions of the Cybersecurity Act are about:

- the importance of developing one's own digital technologies (startups, small and medium-sized enterprises), reducing dependence on foreign suppliers (item 3);
- formation of a competitive environment in the field of electronic communications, provision of information protection and cyber protection services, development of the internal market (items 4-5, 42);
- issues related not only to security technologies, but also to the category of human security (items 50-51).

In its nascent stage, the European models of PPP were defining certain motivational aspects for the establishment of cooperation. It should be noted that more than one reason is usually established to set up the CPPP, but we will consider the following:

- Regulatory requirements. In most cases, PPP in the field of cyber security includes the creation of regulatory requirements, or rather the development of a special law on PPP, which should already contain provisions on cybersecurity issues.
- Economic interests. The authority responsible for a PPP in the sphere of cyber security usually has to minimize obstacles for the development of the industry, ensure the access of ICT products to foreign markets. This may also concern legislative aspects and budgets, in order to adjust the burdens on the private sector and the state. The attraction is enhanced by the fact that the products are of adequate quality, as this can be guaranteed by government.
- Public relations. This aspect is a strong motivation for both participants in the process due to the opportunity of the private sector to participate in the creation of regulatory and legal documents, strategies, as well as to join the base of the public sector and to get confidential information. On the other hand, government bodies get the opportunity to access the ICT products, including Big Data, AI, HPC – supercomputers, etc., as well as they can see solutions, skills and, accordingly, greater understanding of critical infrastructure information protection (CII).

Taking into account the reasons for establishing cooperation, it is also worth noting that cooperation at the initial stage can exist as: Top Down (firstly there must be a strategy or legislative document); Bottom Up (the initiator community); Top Down then grown Bottom Up (there is some kind of strategy, but in the future the leading implementer is the private sector); Bottom Up then grown Top Down (an initiative from private entities that turn to state bodies, the latter take on a greater role in establishing the CPPP); Fire and Forget (a central body, creates a structure for the partnership, but once the partnership is established, provides autonomy); Split or merge (in the

beginning there is some restructuring due to the division into two or more subgroups, but when the relationship and the authority are established, they can unite).

Cultural and political differences are among the most important factors influencing the type and process of PPP model establishment, therefore, there is no common decision. In some countries, formality is an essential part of a PPP, while in others pragmatism will be important. In countries with a strong centralization of state administration, there will be a distance between PPP sectors, which is explained by the hierarchy of power and reluctance to assume authority. There is also a second approach, where states with a certain distribution of power will be more pragmatic and opened for establishing cooperation. Accordingly, these are more individual cases about a national issue.

ENISA researches: Good Practice Guide on Cooperative Models for Effective PPP and Public Private Partnerships (PPP) - Cooperative models identifies 4 types of PPP: institutional, goal-oriented, service outsourcing, hybrid.

Institutional PPP – this type of partnership has the main goal of protecting critical infrastructure, which is implemented due to a certain law with mentioning institutions that have to provide cyber protection of the CIF (critical infrastructure facilities). By this way the basis for cooperation is created, as state actors must take into account the needs, opportunities and challenges of private partners. This is explained by the fact that the private sector has more connections with the real situation in sphere of cyber security regarding CIF. The constant communication is explained by the fact that the parameters of reporting established by law can be limited. Such a PPP model depends on the motivation of civil servants to take cooperation responsibilities and to monitor the situation. The institutional PPP is regulated hierarchically and includes certain national competent authorities responsible for the protection of CIF, as well as cyber security agencies, law enforcement bodies and the academic community that develops support projects. The government allocates money from the budget for the work of the responsible body, which is entrusted with the task of protecting critical infrastructure, but usually does not allocate enough money to provide the services necessary to protect critical infrastructure. The rest of the community contributes to the PPP through voluntary contributions. Examples of successful cases of Institutional PPP are - Information System Administration (Riigi Infosusteemi Amet, RIA) in Estonia, CERT Estonia is part of RIA. Legislation regulates the activity due to the Estonian Emergency Act of 2014 [*Emergency Act*]. And the second example is Poland, the Government Security Center (Rządowe Centrum Bezpieczeństwa, RCB), an institution functions on the basis of the Crisis Management Act (Article 10), and responsible for the management and protection of critical infrastructure [15].

Goal-oriented PPP. This development model is created to achieve a specific goal, more often economic, and focused on providing strategic leadership, giving consultations about innovation to the government. The main participant is the cybersecurity community, including companies, CIF operators, and it generates the initiative, expressing its needs and requests for help to the state. The goal-oriented PPP usually implements management through the head, co-head, and support functions through the secretariat. Activities are done due to budgetary funds and mandatory payments that depend on the type of initiative participant. Examples of such a PPP model is 6 initiatives. Cyber Growth Partnership (CGP) in the UK, where the initiative was launched by the private sector and the condition for participation is that the company can have a large market presence and investment in cybersecurity, so the membership list is updated every year. The co – chair is provided by the minister and the Director – General of a large private entity, the board is provided by representatives of the private sector and the secretariat is provided by the government. Security Made in Luxembourg (SMILE), launched by the Ministry of economy and run by the state, the board and President provide the government, the private sector provides specific services to implement the provisions of legal acts. The joint rule is ensured by minister and director general of a big private entity, rule is ensured by representatives of private sector, secretariat – by government. Security Made in Luxemburg (SMILE) was set up by Ministry of Economy and is ruled by country, the rule and the President ensure the government, the private sector provides certain services for implementation of legal acts. Also, in Austria, the government controls the cybersecurity platform

(CSP) represented by the secretariat, there are representatives of the Federal Chancellor. The cybersecurity council in the Netherlands is an official independent consultative council (ruled by both the public and the private sectors) and its main task is to monitor the implementation of the cybersecurity strategy. The Slovak cybersecurity commission (CSC) is an consultative body of the director of the Office of national security. Spanish industrial safety technology platform – is a private sector association dedicated to protecting CIF. AEI Ciber seguridad y Tecnologia Avanzadas leads the industry and helps cybersecurity companies to promote their services to the market and receive funding from EU programs. Both platforms are entirely managed by private entities.

Service outsourcing PPP – this is when the government recognizes the needs of the industry, but does not have enough resources, so the goal of outsourcing cybersecurity services is to raise awareness among the community. The rule is provided by the private sector through the organization and there is a principle of consensus in decision-making, or the secretariat is the government and decisions are made by the private sector. This type is funded by mandatory contributions and government subsidies, but it is difficult for companies to argue why they should pay contributions to the PPP. Kuratorium Sicheres Österreich (KSÖ) in Austria was established by the Ministry of the interior, since 2010 it is independent and implements a national dialogue on cybersecurity. In cooperation with the industrial sector in 2018 it initiated the "Digital Security Platform". Up KRITIS in Germany is a platform of CIF and the state that includes about 500 organizations.

Hybrid PPP is a partial merger of two PPP models: cybersecurity outsourcing and institutional PPP. Hybrid PPPs are related to the provision of services, and therefore CSIRT is responsible of implementation. It is interesting that the security service is transferred to a private company and this can be said about the government CERT (Gov.CERT) In Austria, where the head is the director of one of the Departments of the Federal Chancellor, and all the functionality is provided by a private company. CSIRT.CZ is managed by CZ.NIC, which is a non-profit organization. Such national CSIRT groups are groups that have received a mandate from the government. Governmental CSIRT groups are usually created to protect the Cyberspace of government agencies. Funding depends on the structure. For example CZ.NIC has an entry fee starting from 1,000 euros and allocates part of this money to CSIRT. The Austrian Gov.CERT is funded by the Chancellor and participation in the PPP is free of charge.

That is why, a cursory analysis shows that making a trustable relationship between public-private, private-private, and public-public partners is a problem when a PPP model creates, and there is no unified standard model.

The importance of implementing the CPPP model in Ukraine is argued by the specifics of this area. Firstly, cyber security is one of the spheres of national security, which deals with the private sector because of the issue of protection of critical infrastructure facilities (CIFs) and critical information infrastructure facilities (CIIFs). The building of relations, legal basis and platforms for the implementation of the CPPP is relevant today because of the intensification of the Russian Federation's actions in cyberspace, as well as because of the growing participation of activists, public structures and representatives of the IT business. The second argument indicates that the leading role and expertise in cyberwar issues are provided by representatives of the non-state sector. The most observed participation of representatives of the red team and pentesters, that both can be classified as – "Grey hat". They do not have a negative impact on the system, unlike "Black hat", and what is currently positive for activists is that at least in March 2022 the Criminal Code of Ukraine was amended. According to the amendments, the bug bounty of state information systems is legal. It is currently necessary to involve specialists in cyberspace defense who should also understand the process of dialogue with the authorities, because cyberspace, in fact, eliminates the difference between a private and a state entity. Anyway, the hacking of CIF, CIF or data of a state institution can have devastating consequences for national security.

It is worth mentioning the Global Cybersecurity Index implemented by the ITU, which has 5 assessment indices (criteria), which are legal measures, technical measures, organizational

measures, capacity development, and cooperation. We should pay attention to the 5th one - cooperation, that PPP includes too. The Global Cybersecurity Index for 2020 covers more than 160 countries with a clear geographical distribution, and here Ukraine has a total of 65.93, and for cooperation 12.87 out of 20 points, one of the lowest ratings of European countries. Only the Balkan states have lower indicators. Talking about close and friendly Poland, we can notice it has 93.86 and 20 for cooperation. The Russian Federation is 98.06 and 20 points [*ITU, 2020*]. According to the ITU rating, the problem of the asymmetry of forces in the cyber area and the question whether the Ukrainian cyber security system is still stable arise. The low level of CPPP in Ukraine is one more factor of the relevance in providing its own model of PPP in the field of cyber security.

A fundamental problem of the Ukrainian legal field is weaknesses in the wording (low clarity, gaps, overlapping, misleading, etc.) used to describe the tasks/functions of each state body. Our task is not to analyze the position of all the main subjects of cyber security of Ukraine, but taking into account the 3 structures of the State Service for Special Communications and Information Protection SSSCIP, the Ministry of Digital Transformation (MDT) and the National Coordination Center for Cyber Security at the NSDC. It can be concluded that SSSCIP and MDT have the biggest amount of terms overlapping. Especially it concerns terms of functioning. It is not clear who is responsible and for what. If we turn to the Law of Ukraine On Public-Private Partnership, we will notice it does not have provisions about the implementation of the CPPP, but the Law of Ukraine On the Basic Principles of Cyber Security in Article 10 talks about how public-private interaction should be implemented. This creates a legal vacuum again, because of uncertain understanding the definitions "partnership" and "interaction". 11 provisions of Article 10 of this Law outline the ways and means of this interaction [*Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy*]. Taking into account that MDT is not specified as the main entity of the national cyber security system, some provisions on public-private interaction clearly indicate the functionality of the MDT. Therefore, this may be the first case on the way to the separation of responsible persons for the CPPP in Ukraine – further development of the main law on cyber security, defining the definitions of "interaction" and "partnership", as well as the development of a special act on the CPPP with the definition of the responsible parties.

Currently, we can see that these 3 entities SSSCIP, MDT and NSDC sign contracts about cooperation with states, agencies (for example, SSSCIP entered into a contract with the Department of National Security of the United States of America (CISA) in July 2022). MDT focuses on large industrial IT companies and NSDC conducts meetings with governmental structures of countries friendly to Ukraine. For example, CCDCOE, NATO. However, the problem of who should coordinate the model of the CPPP in Ukraine exists. In addition to the recommendation of the NISD publication [*Dubov, 2018: 75-81*] another option for the development of the CPPP is proposed. As the NSDC according to its Regulations, is responsible for the coordination and control of the activities of security and defense sector entities that provide cyber security [*Polozhennia pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky],* we can understand that it is this body that should undertake the initiation of the platform for the CPPP. The argument for giving a coordinating role to this body can be that according to most PPP models in Europe and according to the list of Network of National Coordination Centers [16], it is the government bodies entrusted with the functions of defense and the implementation of state policy in the field of security that are the leading structures and the responsible subjects in the future. That is why it is suggested to start the initiative from up and choose the "Hybrid PPP" model. With regard to the case of the activation of the cyber community with the beginning of a full-scale war, the motivation of the private sector is already available due to the context of the war and Ukraine has a wide range of representatives from the IT army, communities of Ukrainian hacktivists (for example, Ukrainian Cyber Alliance) to manufacturers of solutions and products, and most professionals are really interested in engaging in communication with the authorities to develop new regulations, strategies, and currently to protect themselves in the legal field through actions in cyberspace. According to the activation of the cyber community with the beginning of a full-scale war, the motivation of the private sector exists already

due to the context of the war and Ukraine has a wide range of representatives starting from the IT army, communities of Ukrainian hacktivists (for example, Ukrainian Cyber Alliance) to bodies that have right to make decision and produce products. Majority of the professionals are really interested in participation in communication with the authorities to develop new regulations, strategies, and currently to protect themselves in the legal field through actions in cyberspace. Probably the secretariat of the future platform can consist of representatives of specialized departments of the main cyber security entities. It should be ruled by NSDC and a representative from the private sector. According to the wide range of the cyber community, a certain consultative group should be created from representatives of various sectors of the IKT market of Ukraine. Understanding the budgetary and resource capabilities of the state, among the main revenues from the budget, according to the European analogy, there should be mechanisms for membership contributions to the platform, taking into account the type and size of the private entity. Periodic consultation with all community stakeholders should be ensured according to the motivation of the private sector. Currently, an example of a platform for the exchange of views is the National Cyber Security Cluster, which is organized by NSDC in cooperation with the US Civilian Research and Development Fund with support of the US Department of State CRDF Global. Due to this, representatives-partners from the state (including representatives of the defense sector and security), private companies (for example, Yegor Aushev - the founder of Cyber Unit Technologies) join the academic community and international partners (representatives of NATO, CISA). The national cluster has already put on the agenda the issue of best practices in the field of CPPP. It should continue the discussion in order to accelerate the process of forming the CPPP. The motivation for the private sector will also be the possibility of access to the development of future cyber security strategies and of giving recommendations about the improvement and development of regulatory and legal acts. This common work on a strategic document will make possible to create a "Strategy of public-private partnership in the field of cyber security" or a conceptual document. Existence of a legal framework will allow each involved party to know exactly its role, responsibilities and what contribution is expected.

Conclusions. Despite the fact that the CPPP is a mutually beneficial form of partnership for both sides – the public and private sectors, in the European area there is a fragmentation of approaches to the development and functioning of the CPPP structure. This occurs because of many factors. All countries in the European area have their own unique aspects of the CPPP, but they are united by the general idea that the CPPP is a basic element for increasing the persistence and development of cyber defense of all subjects. Issues of trust and control are the most essential problems, as well as the ongoing dilemma of whether these structures will be effective in case of massive cyberattacks. There is no European country that has the unique experience of cyberattacks combined with classic military methods and that has a high level of civil society involvement. Thus, taking into account the unique political experience and cultural heritage of each state, we cannot expect the adoption of a certain practice of establishing PPPs in the field of cyber security. Currently, only basic legal acts needed for creation a legal base for the CPPP (with a number of controversial, abstract provisions) have been adopted in Ukraine. Although both the private sector and the public sector demonstrate significant potential for the creation of a national system of CPPP.

References

1. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union [Electronic resource] / EUR-Lex (Web page). – Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

2. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

[Electronic resource] / EUR-Lex (Web page). – Access mode: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

3. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS A Digital Single Market Strategy for Europe [Electronic resource] / EUR-Lex (Web page). – Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52015DC0192

4. COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry [Electronic resource] / EUR-Lex (Web page). – Access mode: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0410

5. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance) [Electronic resource] / EUR-Lex (Web page). – Access mode: https://eur-lex.europa.eu/eli/reg/2019/881/oj

6. Emergency Act [Electronic resource] / Riigi Teataja (Web page). – Access mode: https://www.riigiteataja.ee/en/eli/525062014011/consolide

7. Zakon Ukrainy Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [Electronic resource] / Verkhovna Rada Ukrainy, Zakonodavstvo Ukrainy (Web page). – Access mode: https://zakon.rada.gov.ua/laws/show/2163-19#Text)

8. Polozhennia pro Natsionalnyi koordynatsiinyi tsentr kiberbezpeky [Electronic resource] / Verkhovna Rada Ukrainy, Zakonodavstvo Ukrainy (Web page). – Access mode: https://zakon.rada.gov.ua/laws/show/242/2016#Text

9. Clinton Larry. A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense. // Journal of Strategic Security. – 2011. Vol. 4, no. 2. – P. 97–112.

10. Public Private Partnerships (PPP) 2017 [Electronic resource] / ENISA (Web page). – Access mode: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

11. Global Cybersecurity Index 2020 [Electronic resource] / ITU (Web page). – Access mode: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

12. Dubov D. Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyi dosvid ta mozhlyvosti dlia Ukrainy : analit. dop. / za zah. red. D. Dubov. – K. : NISD, 2018. – 84 s.

13. The Digital Services Act package [Electronic resource] / European Commission (Web page). – Access mode: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

14. The NIS2 Directive: A high common level of cybersecurity in the EU [Electronic resource] / Think Tank European Parliament (Web page). – Access mode: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333

15. Rządowe Centrum Bezpieczeństwa [Electronic resource] / Gov.pl (Web page). – Access mode: https://www.gov.pl/web/rcb/o-rcb2

16. National Coordination Centres [Electronic resource] / European Cybersecurity Competence Centre and Network (Web page). – Access mode: https://cybersecurity-centre.europa.eu/nccs_en