УДК 339(4):334.723:[316.774.004.056]

Frolova Oksana
Ph.D., Associated Professor,
Department of International Information,
Institute of International Relations,
Taras Shevchenko National University of Kyiv,
Ukraine, 36/1 Y. Illienka
E-mail: sancha279@ukr.net
ORCID: https://orcid.org/0000–0001–7105–2762
DOI: http://dx.doi.org/10.18524/2707–5206.2021.34.237903
Kuchmiy Olena
Ph.D., Associated Professor,
Department of International Information,
Institute of International Relations,
Taras Shevchenko National University of Kyiv,
Ukraine, 36/1 Y. Illienka
E-mail: o_kychmiy@ukr.net
ORCID: https://orcid.org/0000–0002–2634–4114
DOI: http://dx.doi.org/10.18524/2707–5206.2021.34.237903

PUBLIC-PRIVATE PARTNERSHIP IN THE SPHERE OF CYBERSECURITY AS AN IMPORTANT FACTOR OF EUROPEAN STABILITY

The article is devoted to the analysis of the benefits and challenges of public-private partnership in the sphere of cybersecurity. Information technologies play a dominant role in the development of modern society. However, rapid progress in this area is closely linked to the emergence of more sophisticated, innovative threats. The information security system, which has developed within the framework of the modern world order, is one of the "pillars" of international stability. Therefore, it became necessary to distinguish cybersecurity as an important component of public life. The state has a particularly important role to play in the information and cybersecurity system, as it can take a number of organizational and technical measures to protect its information space. The article emphasizes that it is possible to reach significant success only by involving the private sector. There are many examples and confirmations of it in the world. Public-private partnership is one of the potential forms of effective cooperation between the representatives of public and private sectors. The overall goal of participating in PPPs, both private and public, is to increase cybersecurity. There is an obvious need to combine the capabilities, potential, experience, technical support and funding of the public and private sectors to combat cyber threats. Each country is trying to find its own way in building a PPP, but such a partnership has already become a new effective mechanism to meet the challenges and threats in today's information society. The article explores the examples of public-private partnership in the sphere of cybersecurity in the EU.

Key words: public-private partnership, cybersecurity, international security, EU.

Introduction

Threats and risks to the modern world order are increasingly the subject of discussion by international actors at high-level meetings, conferences, summits, and for the preparation of various analytical reports. Global problem researchers are trying to predict the potential risks to the international community in order to find the best solutions to avoid them or effectively counteract the negative effects. As the modern world is defined by many experts as post-industrial or informational, innovative, digital, the risks associated with building an information society and information security are particularly actual: artificial intelligence invention and potential threats, invasion of privacy and confidentiality violations, manipulation of public consciousness, information wars, cybersecurity, information overload or information crisis, child safety in the Internet...

These and related issues were raised at the G8 Meeting in Okinawa (Japan, 2000) and formed the basis of the Okinawa Charter of the Global Information Society, during the World Summit on the Information Society (Geneva, 2003; Tunis, 2005), World Economic Forum (Annual Meeting in Davos, Switzerland).

The information security system, which has developed within the framework of the modern world order, is one of the "pillars" of international stability. Information security threats are considered in the context of threats to international security system. Since international security is a fundamental basis for maintaining the stability of the world order as a whole, its formation and consolidation is an essential condition for human existence. International governmental organizations are the main guarantors of the worldwide information security system. The UN, NATO, EU information security concepts lead to common solutions to counteract information and communication threats, prioritize security institutions to develop a common international information security strategy, combat cyberwarfare, information terrorism and combat crime. Non-governmental non-profit research organizations such as the Club of Rome and RAND are developing solutions to address the challenges of international and national information policy. In addition, there are international organizations and forums of practical orientation that are intended to bring to life various information and cybercrime prevention projects. For example, FIRST is a leading international organization and a recognized global leader in cyber security incidents. More than 500 teams from 94 countries are members of the organization.

But the state has a particularly important role to play in the information and cyber security system, as it can take a number of organizational and technical measures to protect its information space. The state is the guarantor of ensuring national security in general and information as its important component in particular. Information security ensures the integrated interaction of all elements of the system within the general concept of state security. The basic laws of many states claim that protecting the sovereignty and territorial integrity of countries, ensuring its economic and information security are the most important functions of the state.

As the cybersecurity field is extremely dynamic and innovative, such a fundamental and conservative subject of international relations as a state is simply unable to respond quickly and effectively to new challenges without the assistance of the private sector and public organizations. The involvement of the state in creating systemic organizational decisions and legal framework for combating cyber threats is insufficient. It is possible to reach significant success only by involving the private sector. There are many examples and confirmations of it in the world. Public-private partnership (PPP) is one of the potential forms of effective cooperation between the representatives of public and private sectors.

Today, public-private partnership is recognized as a key element in building a truly effective cybersecurity system. Even the rating of the International Telecommunication Union "Global Cyber Security Index" already has a graph and takes into account such an indicator as public-private partnership. The purpose of the study is to explore the benefits and challenges of public-private partnership in the sphere of cybersecurity and to highlight the already existing positive experience of EU member states as an example for improving the level of cybersecurity for other countries through the development of PPP. The theoretical overview includes basic and current authors, administrative documents, documents of international and national organizations, papers and reports.

Among foreign researchers on understanding the benefits and problems of PPP worked actively S. Linder, M. Kostiainen, A. Jagasia, V. Kouwenhoven, R. Wettenhall, T. Moore, M. Carr and others. For example, Stephen Linder describes that the purpose of the PPP is to use synergies in the innovative sharing of resources and management knowledge to optimally achieve the goals of all parties involved, if these goals could not be achieved without the involvement of these parties (Linder, 2000).

Vincent Kouwenhoven notes that PPP is impossible without mutual trust and restrictions to prevent abuse; risk distribution; availability of clear, unambiguous goals and strategies; responsibilities, powers, and functions of ensuring partner business interests (Kouwenhoven, 1993).

In Ukraine, the problem of PPP was studied in detail by researchers at the Institute for Strategic Studies: V. Boyko, D. Dubov, S. Hnatyuk, T. Isakova, M. Ozhevan, A. Pokrovska. The normative-legal and organizational bases of public-private partnership in Ukraine are considered in the work, effective examples of such partnership are given. Perspective directions of development of cybersecurity public-private partnership in Ukraine and possible ways of their implementation are outlined (NISS, 2018).

Benefits and Challenges of PPP

The most common causes or drivers of PPP creation are:

• Economic interests as a common motivation for engaging the private sector. It may be a desire to create a body that will help to identify barriers to the growth of the cybersecurity industry and create the conditions for exporting cybersecurity products.

• Legislation requirements. For example, PPPs are created as an implementation of a specific law, the requirements of which can be better implemented within the PPP. This is often the case of crisis management or emergency situations. Mostly, this kind of legislation applies to PPP in general, not just cybersecurity. It was created to stimulate the economy, but as cybersecurity becomes an increasingly important political issue, PPPs also focus on cybersecurity.

• Public Relations. In this case, the government allows the private sector to contribute to new legislation and to work together to develop a national cyber security strategy. For the private sector, motivation is to engage with the government and other private knowledge-sharing structures.

• Social interests. When social interest was called a driving force, it was usually the motivation for broadly discussing of cybersecurity in the country and establishment of cyber security at a high level on the political agenda. It is important for the industry the promotion of cybersecurity in general and its smooth development.

• Other reasons. There are also other reasons for establishing PPP. Experts include the new EU regulations (the NIS Directive and the General Data Protection Regulation), which set new requirements for the private sector. For this reason, governments decide to create PPPs to help the industry to apply the new rules.

It should be noted that there are often several reasons for creating PPP. The most common scenario is that there are economic and social interests that are accompanied by new regulation. This requires an exchange of information and cooperation between private and public entities (ENISA, 2017).

The overall goal of participating in PPPs, both private and public, is to increase cybersecurity. However, there is also a number of different motivations and reasons why partnership can be beneficial to public and private entities and which may be common benefits of PPPs. For example, for state structures, the main reasons may be the limited implementation of state strategy tools; the national security strategy should include the involvement of non-governmental companies; the government lacks sufficient funds to engage all small stakeholders in critical infrastructure protection; a better understanding of the security of information about critical infrastructure; the ability to build links between various private sector initiatives; access to private sector resources (such as valuable experts) to facilitate standard-setting.

For private companies, the main reasons may be: going out the solution of the problem beyond the organizational capabilities of the company; lack of involvement of senior executives to the action; the ability to influence the future national security strategy; interest in effective mechanisms of neutralization of inadequate state regulation; access to public funds; the ability to influence national legislation and mandatory standards; confidence in the products and services supplied through PPP, as guaranteed by the government.

For the common benefit, the main reasons may be: the desire to eliminate the vulnerability of previous negative experience; failure to provide some or all stages of the security life cycle; the evolution of threats from national to

international; lack of trust between competitors within geographical, sectoral or thematic areas, and therefore there is a need to create a trusted structure to solve the problem; exchange of knowledge, experience and best practices; achievement of stability of the cybersystem; establishing direct and reliable contacts with other organizations.

Despite the obvious benefits and effectiveness of PPP, it is an extremely complex and ambiguous phenomenon that has many problems and challenges:

• The lack of trust between the public-private, private-private and public-public entities. Most PPPs define trust as an ongoing process that involves a personal relationship and takes a long time. During PPP service, the trust can be lost if a new member joins or there are inactive members. The best mechanisms to support and build trust can be face-to-face meetings, regular meetings, social events, thematic conferences and trainings.

• Lack of human resources in both the public and private sectors. Insufficient allocation of human resources for the development of PPP is considered to be the main problem. Governments usually do not attract enough people because they do not consider PPP a priority, and the private sector usually directs its best human resources to do business and profit.

• Insufficient funding. Lack of budget and resources in the public sector is one of the key problems for PPP. Governments often do not provide sufficient funds for PPP development, and do not budget them in advance for the future. At the same time, the public sector is considering a long-term perspective when developing a PPP strategy and action plan. On the other hand, the private sector operates in a dynamic framework, which means that strategies and action plans can be created only for a few years.

• Low level of general understanding and dialogue between the public and private sectors. It is very difficult to create a common language for clear PPP communication. Different organizations use different language. Lack of general perception of things can create misunderstandings that are difficult to resolve. It is difficult to gain a common understanding of how the private and public sectors work. Such concepts as “strategic”, “operational” and “technical” can mean very different in different work environments and cultures.

• Weak involvement and promotion of the concept of PPP among small and medium-sized enterprises (SMEs). SMEs usually do not have the resources or relevant experience to participate in PPP. Encouraging of SMEs to participation can be beneficial for them as they will gain experience from big players.

• Lack of guidance and legal framework. Indecision about leadership and government disinterest prevents private sector participation. Exchange of knowledge, experience and active participation in discussions contribute to the effective development of PPP. In addition, the private sector is sad to point out the discrepancies between key government agencies and delays in decision-making. The private sector expects active action from the government. Legal framework will allow each of the involved parties to know exactly what their role and responsibilities are, what contribution should be made and what benefits should be expected (ENISA, 2017).

European Experience of PPP in the Sphere of Cybersecurity

EU Member States are particularly active and successful in the field of PPP. Of course, the basis of any progress at the national and international level is the legal framework. With the adoption of the document "i2010 — A European Information Society for growth and employment" of 2005 (EUROPEAN COMMISSION, 2005). and "A strategy for a Secure Information Society — Dialogue, Partnership and Empowerment" in 2006 (EUROPEAN COMMISSION, 2006). The European Commission emphasized the importance of network and information security (NIS) and the desire to create a single European information space. The documents stress the importance of dialogue, partnership and empowerment of all stakeholders for properly threats response. European Cybersecurity is based on the European Union Cyber Strategy 2013, the Digital Single Market Strategy 2015 and the EU Network and Information Security Directive 2015. The European Commission's Critical Information Infrastructure Protection (CIIP) document (2008) proposes specific policy and regulatory provisions for improving the security and resilience of public telecommunications including the creation of a European Public Private Partnership for Resilience (EP3R) + (ENISA, 2008).

In 2013 the European Commission presented the European Union Strategy for Cybersecurity: open and secure cyberspace (EUROPEAN COMMISSION, 2013). The document outlines the EU's approach to preventing and responding to cybercrime, and stresses that fundamental rights, democracy and the rule of law must be protected in cyberspace. It was the first strategic document at European level that concerned only cybersecurity. The strategy recognizes that achieving cybersecurity is a strategic priority, and effective cooperation between public authorities and the private sector is extremely important.

Information and communication technologies have become the base of economic growth. They are an important resource for all economic sectors. Information and communication technologies are at the heart of complex systems that support the economy in key sectors such as finance, health, energy and transport. Many business models are built on the uninterrupted availability of the Internet and the steady functioning of information systems. Most of these systems are under the control of the private sector that is why it is extremely important for governments.

The EU Cybersecurity Strategy 2013 encouraged pan-European discussions about the necessity of public-private cooperation in cybersecurity.

The Digital Single Market Strategy (2015) contains a number of initiatives that are designed to open up digital opportunities for society and business and support Europe's position as a global leader in the digital economy. As the DSM strategy emphasizes the role of the digital economy, it concerns the private sector and its interaction with public administration. Building a Digital Single Market in Europe requires effective collaboration between industry and government. Particular emphasis in the Strategy is on the mutual understanding of needs and constraints, which is vital (EUROPEAN COMMISSION, 2015).

Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and in-

formation systems across the Union ("NIS Directive") was adopted in 2016 (EU, 2016). Implementation of the Directive on the activities of the high security of network and information systems can be a huge challenge for Member States, but PPP can support this process. The Directive proposes to increase the level of cybersecurity awareness between citizens and essential service providers, since only a sufficient level of knowledge about cyber threats can improve the overall level of cybersecurity in Europe. This can be achieved through a PPP that allows sharing of knowledge, best practices and creating a common level of understanding between all stakeholders. Directive 2016/1148 also refers to the establishment of cooperation between national competent authorities and operators of essential information services, which is also impossible without close cooperation.

In September 2017, the European Commission presented a joint document on resilience, deterrence and defense: building strong cybersecurity for the EU. It is intended to building a strong single market through the EU's cybersecurity certification system, by creating an operational cybersecurity plan, by investing in secure encryption and protection of fundamental rights, by enhancing the role of ENISA and developing international cybersecurity cooperation (EUROPEAN COMMISSION, 2017). The document emphasizes the importance of cooperation and confidence building through public-private partnerships. The European Commission will continue to support the establishment of public-private partnerships and cooperation mechanisms, as this will be a further step to strengthen the EU's cybersecurity capabilities through the network of cybersecurity centers which are based on the European Cybersecurity Center.

The European Union Agency for Network and Information Security (ENISA) became one of the first international organizations which began to research the need of PPP. ENISA is a center of network and information security for the EU and its Member States, the private sector and EU citizens. The organization works with these groups to develop advice and recommendations on good practice in the field of information security. In 2011, ENISA experts said in their study "Cooperative Models for Effective Public Private Partnerships Good Practice Guide" that public-private partnerships have progressed in many Member States and at different times, depending on the environment, culture and legislation. It is therefore not surprising that there is no general definition of what PPP is. But the experts described their PPP as "An organized relationship between public and private organizations, which establishes common scope and objectives, and uses defined roles and work methodology to achieve shared goals" (ENISA, 2011). The need for a European perspective is demonstrated by the emergence of the European Public Private Partnership for Resilience (EP3R), which is working with national PPPs to address critical information infrastructure protection issues at European level. There is also a need for international cooperation. No country can create a strategy to protect critical information infrastructure in isolation, as there are no national borders in cyberspace. The survey collected questionnaires from the public and private sectors in 20 countries, which provided answers to the key questions:

why PPP is needed; who should it involve in the process; how should it be governed; what services and incentives should be offered; when should action be taken to start it and maintain sustainability. The guide highlights recommendations, observations and offers quotes from interviews (ENISA, 2011).

ENISA experts offer three basic PPP models:

1) PPP focused on response. Mainly operational and tactical groups that deal directly with the consequences of the attacks;

2) PPP focused on prevention. The main purpose is to prevent and avoid attacks. To a greater extent, strategic groups that have significant mutual trust, formed through years of experience;

3) "Umbrella" PPP. Structures try to cover all the elements, from preventative measures to crisis relief. It is required a high level of readiness for cooperation partners.

In 2018, ENISA experts have prepared a new research: Public Private Partnership, Cooperative models which analyzes the state of PPP within the EU. The study notes that the cultural dimension is one of the most important determinants of the development of public-private partnerships that are developing in Europe. Due to cultural differences, there is no universal scenario for creating a successful PPP. The model applied in one country will not be necessarily successful in another. The study also identified other problems and difficulties for PPP in the EU: lack of human resources in both the public and private sectors; insufficient budget and public sector resources do not meet the expectations of the private sector; insufficient establishment of a common level of understanding and dialogue between the public and private sectors; lack of leadership and legal framework. The basic principles for creating a PPP ecosystem in Europe are to provide the proper human resources and to create the legal foundations for cooperation. It is also important to ensure open communication between the public and private sectors. The involvement of small and medium-sized enterprises in the process of PPP development is crucial, as they are the backbone of the European economy.

The analysis of the current state of PPP within the EU lists the most active actors: private service providers (17 %), cybersecurity agencies (16 %), research organizations (16 %), national competent authorities (14 %), law enforcement agencies (12 %), national intelligence agencies (7 %) (ENISA, 2017).

A new ENISA 2018 study identifies new possible PPP models:

1) Institutional PPP. In this model, all institutions operate within the general rules of PPP. As a rule, this type of PPP provides numerous services. For example, incident response and crisis management, research and analysis, development of best practices and recommendations, exchange of information, early incident prevention, awareness raising, technical assessment, standard setting, strategic planning, risk analysis. This type of PPP is often associated with critical infrastructure protection. Collaboration between PPP participants in this model is organized as working groups, rapid response groups and long-term associations. The main goal is to secure critical infrastructure in general, but with a focus on cyber-security;

2) Goal-oriented PPP. It is usually built when additional support from the government is required. This type of PPP is focused on delivering strategic solutions, supporting the IT market and creating a framework for cybersecurity in the country. Goal-oriented PPP s and their specifications most reflect the cultural differences between Member States. Similar goals are achieved by very different approaches. PPPs of this type are created to build a cybersecurity culture in EU Member States. Goal-oriented PPP s play an important role in providing strategic planning and advising governments on innovation; providing guidance on the creation of new laws and supporting the development of the cyber security industry. There is usually a platform or council that brings together the private and public sectors to share knowledge and experience.

3) Service outsourcing PPP. PPPs of this type are initiatives created by the government and the private sector to identify problems in a particular industry, but neither party has the resources or the capacity to solve them. Their main task is to raise awareness of cybersecurity among stakeholders. These PPPs can actually be seen as third parties for providing outsourcing services that meet the needs of the industry and support the government in policy-making.

4) Hybrid PPP. Generally speaking, there is a combination of institutional and outsourcing PPP. It occurs when the government lacks the resources needed to secure specific decisions at the national level, so there is a need for co-operation with a private entity with appropriate experience and resources. Most often this activity includes the CSIRTs operating ENISA, 2017).

It is clear that these models of PPP construction are not the only possible ones, but at the present stage a rather comprehensive and practically significant explanation of the formation and implementation of PPPs in the field of cybersecurity is offered. The variability of PPP models in different democracies often depends on both the regulatory space of the countries and the traditions of the PPP that have historically evolved in them (NISS, 2018).

The ENISA report aims at the analysis of the current state of PPP in the EU. The study identifies the main models of cooperation, the current challenges facing both the private and public sectors in the process of creating and developing PPPs, and provides recommendations for the development of PPPs in Europe.

In June 2016, a non-profit European Cybersecurity Organization (ECSO) was created under Belgian law. The organization brings together various European stakeholders in cybersecurity from EU Member States, the European Free Trade Association (EFTA) and countries associated with the H2020 Program. The main objective of ECSO is to develop a competitive European cybersecurity ecosystem, to support the protection of the European Digital Single Market and to promote European digital autonomy. ECSO is a private partner of the European Commission in the implementation of the PPP on cybersecurity (ECSO, 2020).

As part of the EU's cyber security strategy, on 5 July 2016, the European Commission and the European Cybersecurity Organization (ECSO) signed a Public Private Partnership Agreement (cPPP). The purpose of the partnership

is to facilitate cooperation between public and private actors in the early stages of the research and innovation process so that EU Member States have access to innovative European solutions (ICT products, services and software). These decisions take into account fundamental rights such as the right to privacy.

The agreement also aims at stimulating the cybersecurity industry by helping to balance supply and demand sectors as well as sectors that are important users and customers of cybersecurity services (eg energy, healthcare, transport, finance). The agreement also aims to stimulate the cybersecurity industry by helping to balance supply and demand sectors as well as sectors that are important users and customers of cybersecurity services (eg energy, healthcare, transport, finance). A public-private partnership agreement between the European Commission and the European Cybersecurity Organization will help to structure and coordinate industrial digital security resources in Europe. It will include a wide range of actors, from innovative small and medium-sized enterprises to component and equipment manufacturers, critical infrastructure operators and research institutes united under the auspices of ECSO.

The EU is investing € 450 million into this partnership as part of its Horizon 2020 research and innovation program. It is expected that cybersecurity market participants invest three times more (ECSO, 2020). By the way, in April 2019, a new EU Horizon Europe 2021–2027 EU research and innovation program was approved. Among the global challenges and solutions to European industrial competitiveness in the new program are new digital technologies, artificial intelligence, robotics, advanced computing, Big Data, next-generation Internet, data protection and cybersecurity.

Currently, ECSO is working with the European Commission's Joint Research Center (JRC) and other stakeholders to identify common requirements and conditions for cooperation. Recognizing the importance of certification for the development of a strong European cybersecurity market, in 2019 ECSO signed memorandums of understanding with European Standardization Organizations, CEN / CENELEC and ETSI. The purpose of the memorandum is to ensure the standardization of officially recognized European and international organizations as the basis for certification schemes in the field of cybersecurity (ECSO, 2018).

Also in 2019, ECSO signed memorandums of understanding with the 5G Infrastructure Association. The aim is to expand future collaboration on cybersecurity and 5G communications networks. The Memorandum of Understanding formalizes synergies and collaborations in the exchange of information and experience in cybersecurity and 5G to identify priority areas for research, the development of secure technologies and robust platforms, and to prevent technology fragmentation across borders (ECSO, 2018).

In 2019, the European Parliament and the Council of the European Union adopted the EU Cybersecurity Act 2019/881 (EU, 2019). which establishes a new mandate for ENISA, the EU Cybersecurity Agency and establishes a European Cybersecurity Certification System. According to the adopted document, ENISA assumes a permanent mandate, including increasing responsibilities and resources.

At the same time, the European Cybersecurity Certification System establishes rules and regulations for the certification of ICT products, processes and services within the European Union. With the entry into force of the Cybersecurity Act, Europe has been equipped with a full-fledged European Agency and a first certification system across the EU, which provides significant components for a strong European cybersecurity approach in terms of capacity building and market competitiveness.

Most EU Member States have been actively involved in the public-private partnership process in the field of cybersecurity. 16 EU Member States (Austria, Belgium, Bulgaria, United Kingdom, Greece, Estonia, Ireland, Spain, Cyprus, Lithuania, Germany, Poland, Romania, Slovenia, France and the Czech Republic) set up Cybercrime Excellence Centers to facilitate law enforcement cooperation, academic and private partners for the development and exchange of best practices, training and capacity building (EUROPEAN COMMISSION, 2017). According to the International Telecommunication Union, all EU Member States have national Computer Emergency Response Teams (CERT), which are active participants in PPP (ITU, 2018).

The UK, for example, is regarded as a leading progressive country with high levels of cybersecurity. According to the Global Cybersecurity Index 2018 prepared by the International Telecommunication Union (ITU), the United Kingdom is ranked # 1 among 175 countries (Figure 1) (ITU, 2018). Here we can see top 10 countries from the Index. There is no GSI 2019. Due to the COVID-19 the publication of the GCIv4 report is tentatively set for early 2nd quarter of 2021.

Figure 1

Global Cybersecurity Index 2018

Member State	Score	Global Rank
United Kingdom	0.931	1
United States of America*	0.926	2
France	0.918	3
Lithuania	0.908	4
Estonia	0.905	5
Singapore	0.898	6
Spain	0.896	7
Malaysia	0.893	8
Canada*	0.892	9
Norway	0.892	9
Australia	0.890	10

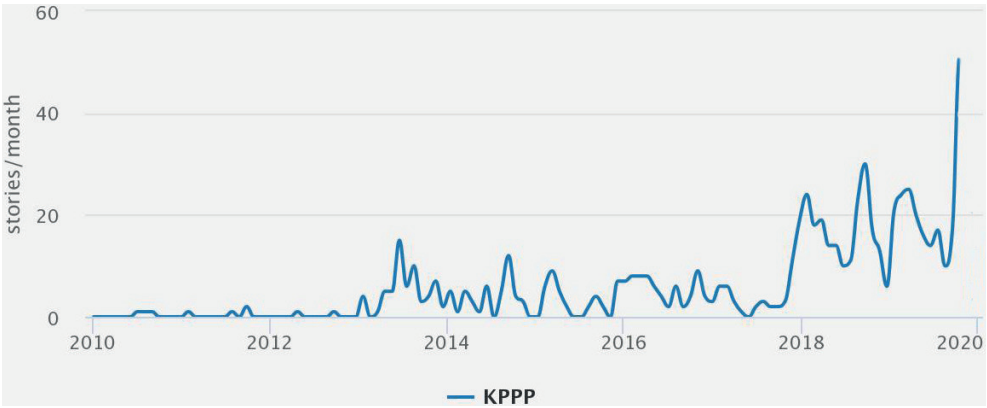
Collaboration is one of the five indicators that have served as the basis for the cybersecurity index, in addition to legislative regulation, technical capacity, organizational work and capacity development. Collaboration includes: public-private partnerships, bilateral and multilateral cooperation, participation of states in establishing international regulatory mechanisms.

Conclusions

The problem of cybersecurity is becoming more urgent and widespread. The content analysis of media monitoring over last ten years (2010–2020) regarding the online platform 'Media Cloud' shows the relevance of the investigated problem (Figure 2).

Figure 2

Total Attention to the Selected Topics over January 2010 — March 2020



Source: compiled by the authors according to online platform 'Media Cloud'.

The overall goal of participating in PPPs, both private and public, is to increase cybersecurity. However, there is also a number of different motivations and reasons why partnership can be beneficial to public and private entities and which may be common benefits of PPPs. For the common benefit, the main reasons may be: the desire to eliminate the vulnerability of previous negative experience; failure to provide some or all stages of the security life cycle; the evolution of threats from national to international; lack of trust between competitors within geographical, sectoral or thematic areas, and therefore there is a need to create a trusted structure to solve the problem; exchange of knowledge, experience and best practices; achievement of stability of the cybersystem; establishing direct and reliable contacts with other organizations.

There is an obvious need to combine the capabilities, potential, experience, technical support and funding of the public and private sectors to combat cyber threats. Each country is trying to find its own way in building a PPP, but such a partnership has already become a new effective mechanism to meet the challenges and threats in today's information society. Each participant in

a public-private partnership has its organizational, technical, financial and intellectual capabilities, which together become a powerful driving force for the development of the cybersecurity sector. Reliable cyber security sector helps not only to protect the state and its citizens, but also becomes a driver of economic growth.

References

Dubov, D. (Ed.). (2018). *Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyj dosvid ta mozhlyvosti dlya Ukrayiny (Public-private partnership in the field of cybersecurity: international experience and opportunities for Ukraine: Analytical Report)*. Kyiv: NISS. [in Ukrainian].

Brooks, C. (2019). Public private partnerships and the cybersecurity challenge of protecting critical infrastructure. Forbes. Retrieved from https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/#67f72ce85a57

Cyber Exchange. (2020). Retrieved from https://cyberexchange.uk.net/#/about

ECSO. (2018). Memorandum of Understanding. Retrieved from https://ecs-org.eu/press-releases/ecso-and-cen-cenelec-sign-memorandum-of-understanding

ECSO. (2020). Retrieved from https://ecs-org.eu/about

ECSO. (2020). Retrieved from https://ecs-org.eu/cppp

ENISA. (2008). 'Stock Taking of Policies and Regulations — Resilience of Communications Networks'. Retrieved from http://www.enisa.europa.eu/act/res/policies/stock-taking-of-nationalpolicies/?searchterm=stock taking

ENISA. (2011). Good Practice Guide on Cooperatve Models for Effective PPPs. Retrieved from https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps

ENISA. (2017). Public Private Partnerships (PPP) Cooperative models. Retrieved from https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport

EU. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ. L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOEU. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council. Retrieved from https://eur-lex.europa.eu/eli/reg/2019/881/oj

EUROPEAN COMMISSION. (2005). 2010 — A European Information Society for growth and employment". Retrieved from https://ec.europa.eu/commission/presscorner/detail/en/MEMO_05_184

EUROPEAN COMMISSION. (2006). A strategy for a Secure Information Society. Retrieved from https://ec.europa.eu/information_society/doc/com2006251.pdf

EUROPEAN COMMISSION. (2013). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Retrieved from http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

EUROPEAN COMMISSION. (2015). A Digital Single Market Strategy for Europe. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A52015DC0192

EUROPEAN COMMISSION. (2017). Joint communication to the European parliament and the council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Retrieved from https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf

EUROPEAN COMMISSION. (2017). Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Retrieved from https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf

Federation of American Scientists (1998). Presidential decision Directive /NSC-63. Retrieved from https://fas.org/irp/offdocs/pdd/pdd-63.htm

HM Treasury. (2012). A new approach to public private partnerships. Retrieved from https://goo.gl/fBj8mF

ITU. (2018). Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIRT_Status.pdf
ITU. (2018). Global Cybersecurity Index 2018. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI. 01–2018-PDF-E. pdf
Kouwenhoven, V. (1993). Public-Private Partnership: A model for the management of Public-Private cooperation. In J. Kooiman [Ed.], *Modern Governance. New Government–Society Interactions* (pp. 119–130). London, Sage.
Linder, S., & Vaillancourt, P. (2000). Rosenau, Mapping the terrain of the Public–Private Policy Partnership. In P. Vaillancourt Rosenau (Ed.), *Public–Private Policy Partnerships* (pp. 1–19). Cambridge, MA: The MIT Press.
National Cyber Security Centre. (2019). The NCSC Annual Review. Retrieved from https://www.ncsc.gov.uk/news/annual-review-2019
National Cyber Security Centre. (2020). Retrieved from https://www.ncsc.gov.uk/
National Cyber Security Centre. (2020). Cyber Security Information Sharing Partnership. Retrieved from https://www.ncsc.gov.uk/section/keep-up-to-date/cisp
National Cyber Security Strategy. (2016–2021). Retrieved from https://goo.gl/QEQs11
PPP Forum. (2020). Retrieved from https://www.pppforum.com/hometechUK Retrieved from https://www.techuk.org/cyber-growth-partnership
The UK Cyber Security Strategy 2011–2016: Annual Report. (2016). Retrieved from https://www.gov.uk/government/uploads/system/uploads/attachment_data/fi le/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf
The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world. (2011). Retrieved from https://goo.gl/XWskxu

Список використаної літератури

Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. /за заг. ред. Д. Дубова. К. : НІСД, 2018. 84 с.
A strategy for a Secure Information Society. European Commission. URL: https://ec.europa.eu/information_society/doc/com2006251.pdf (дата звернення: 14.09.2020).
Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 2013. European Commission. URL: http://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (дата звернення: 14.09.2020).
i2010 — A European Information Society for growth and employment. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_05_184 (дата звернення: 14.09.2020).
Stock Taking of Policies and Regulations — Resilience of Communications Networks. 2008. ENISA. URL: http://www.enisa.europa.eu/act/res/policies/stock-taking-of-nationalpolicies/?searchterm=stock taking (дата звернення: 15.11.2020).
A Digital Single Market Strategy for Europe. 2015. European Commission. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX %3A52015DC0192 (дата звернення: 18.02.2021).
Brooks C. Public private partnerships and the cybersecurity challenge of protecting critical infrastructure. Forbes. URL: https://www.forbes.com/sites/cognitiveworld/2019/05/06/public-private-partnerships-and-the-cybersecurity-challenge-of-protecting-critical-infrastructure/#67f72ce85a57 (дата звернення: 12.11.2020).
Cyber Exchange. URL: https://cyberexchange.uk.net/#/about (дата звернення: 09.02.2021).
Cyber Security Information Sharing Partnership. 2020. National Cyber Security Centre. URL: https://www.ncsc.gov.uk/section/keep-up-to-date/cisp (дата звернення: 15.05.2021).
Directive (EU) 2016/1148 of the European Parliament and of the Council. EU. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ. L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TO (дата звернення: 06.04.2021).
ECSO. URL: https://ecs-org.eu/about (дата звернення: 7.02.2021).
ECSO. URL:: https://ecs-org.eu/cppp (дата звернення: 16.03.2021).
Federation of American Scientists (1998). Presidential decision Directive /NSC-63. URL: https://fas.org/irp/offdocs/pdd/pdd-63.htm (дата звернення: 12.04.2021).

Global Cybersecurity Index 2018. ITU. URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI. 01–2018-PDF-E. pdf (дата звернення: 11.03.2021).
Good Practice Guide on Cooperatve Models for Effective PPPs, 2011, ENISA. URL: https://www.enisa.europa.eu/publications/good-practice-guide-on-cooperatve-models-for-effective-ppps (дата звернення: 12.04.2021).
HM Treasury. A new approach to public private partnerships, 2012. URL: https://goo.gl/fBj8mF (дата звернення: 18.11.2020).
ITU. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIRT_Status.pdf (дата звернення: 11.03.2021).
Joint communication to the European parliament and the council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 2017. European Commission. URL: https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf (дата звернення: 18.02.2021).
Kouwenhoven V. Public-Private Partnership: A model for the management of Public-Private cooperation. Modern Governance / J. Kooiman (Ed.). London: New Government–Society Interactions, Sage, 1993. P. 119–130.
Linder S., Vaillancourt P. Rosenau, Mapping the terrain of the Public-Private Policy Partnership. *Public-Private Policy Partnerships* / P. Vaillancourt Rosenau (Ed.). Cambridge, MA: The MIT Press, 2000. P. 1–19.
Memorandum of Understanding, 2018, ECSO. URL: https://ecs-org.eu/press-releases/ecso-and-cen-cenelec-sign-memorandum-of-understanding (дата звернення: 15.04.2021).
National Cyber Security Centre. URL: https://www.ncsc.gov.uk/ (дата звернення: 15.05.2021).
National Cyber Security Strategy (2016–2021). URL: https://goo.gl/QEQs11 (дата звернення: 15.05.2021).
PPP Forum, 2020. URL: https://www.pppforum.com/home (дата звернення: 9.05.2021).
Public Private Partnerships (PPP) Cooperative models. 2017. ENISA. URL: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport (дата звернення: 15.04.2021).
Regulation (EU) 2019/881 of the European Parliament and of the Council. EU. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj (дата звернення: 11.12.2020).
Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 2017. European Commission. URL: https://www.consilium.europa.eu/media/21479/resilience_deterrence_defence_cyber-security_ec.pdf (дата звернення: 18.02.2021).
techUK, 2020. URL: https://www.techuk.org/cyber-growth-partnership (дата звернення: 9.05.2021).
The NCSC Annual Review, 2019, National Cyber Security Centre. URL: https://www.ncsc.gov.uk/news/annual-review-2019 (дата звернення: 11.03.2021).
The UK Cyber Security Strategy 2011–2016: Annual Report. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/fi le/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (дата звернення: 9.05.2021).
The UK Cyber Security Strategy: Protecting and promoting the UK in a digital world (2011). URL: https://goo.gl/XWskxu (дата звернення: 7.04.2021).

Стаття надійшла до редакції 26.07.2021

Фролова О. М.
кафедра міжнародної інформації Інституту міжнародних відносин
Київського університету імені Тараса Шевченка
вулиця Юрія Іллєнка, 36/1, Київ, 04119, Україна
Кучмій О. П.
кафедра міжнародної інформації Інституту міжнародних відносин
Київського університету імені Тараса Шевченка
вулиця Юрія Іллєнка, 36/1, Київ, 04119, Україна

ДЕРЖАВНО-ПРИВАТНЕ ПАРТНЕРСТВО У СФЕРІ КІБЕРБЕЗПЕКИ ЯК ВАЖЛИВИЙ ФАКТОР ЄВРОПЕЙСЬКОЇ СТАБІЛЬНОСТІ

Резюме

Стаття присвячена аналізу переваг державно-приватного партнерства у сфері кібербезпеки. Інформаційні технології відіграють домінуючу роль у розвитку сучасного суспільства. Однак прогрес у цій галузі пов'язаний з появою більш складних загроз. Система інформаційної безпеки, яка склалася в рамках сучасного світового порядку, є одним із «стовпів» міжнародної стабільності. З'явилася необхідність виділити кібербезпеку як складову суспільного життя. Держава повинна відігравати важливу роль у системі інформаційної та кібербезпеки, оскільки вона може вжити низку організаційних та технічних заходів для захисту свого інформаційного простору. У статті наголошується, що досягти успіху можна, лише залучивши приватний сектор. Державно-приватне партнерство (ДПП) є однією з потенційних форм ефективної співпраці між представниками державного та приватного секторів.

Загальною метою участі в ДПП, як для приватного сектора, так і для держави, є підвищення кібербезпеки. Однак існує ряд причин, чому партнерство може бути корисним і для державних, і для приватних структур. Наприклад, для державних структур причинами можуть бути: обмеженість інструментів реалізації державної стратегії; у стратегії національної безпеки може бути передбачена участь недержавних компаній; відсутність коштів в уряді для залучення малих стейкхолдерів до захисту критичної інфраструктури; системне розуміння критичної інфраструктури, необхідної для захисту інформації; можливість забезпечити взаємозв'язок між різними ініціативами з приватного сектора; доступ до ресурсів приватного сектора, що полегшує встановлення стандартів. Для приватних компаній основними причинами можуть бути: вихід вирішення проблеми за межі організаційних можливостей компанії; брак залученості вищих керівників до дій; можливість впливати на майбутню стратегію національної безпеки; зацікавленість у дієвих механізмах нейтралізації неадекватного державного регулювання; доступ до державних коштів; можливість впливати на національне законодавство та обов'язкові стандарти; впевненість в якості продуктів та послуг, що постачаються через ДПП, оскільки це гарантується урядом. Для спільної вигоди основними причинами можуть бути: бажання усунути вразливість від попередньо пережитого негативного досвіду; наявність провалів у забезпеченні деяких або всіх етапів життєвого циклу безпеки; розвиток загроз з національного рівня на міжнародний; брак довіри між конкурентами в межах географічних, секторальних або тематичних сфер, а отже, існує потреба у створенні довіреної структури для вирішення цієї проблеми; обмін знаннями, досвідом та передовою практикою; досягнення стійкості кіберсистеми; налагодження прямих та надійних контактів з іншими організаціями. У статті доводиться, що існує потреба поєднати можливості, потенціал, досвід, технічну підтримку та фінансування державного та приватного секторів для боротьби з кіберзагрозами. Кожна країна намагається знайти найбільш ефективний шлях у по-

будові ДПП. Надійний сектор кібербезпеки допомагає не лише захистити державу та її громадян, але й стати рушієм економічного зростання. Особливо активними та успішними у сфері ДПП є країни-члени ЄС. Стаття досліджує приклади та особливості державно-приватного партнерства у сфері кібербезпеки в ЄС.

Ключові слова: державно-приватне партнерство, кібербезпека, міжнародна безпека, ЄС.

Фролова О. М.
кафедра международной информации Института международных отношений Киевского университета имени Тараса Шевченко
улица Юрия Ильенко, 36/1, Киев, 04119, Украина
Кучмий О. П.
кафедра международной информации Института международных отношений Киевского университета имени Тараса Шевченко
улица Юрия Ильенко, 36/1, Киев, 04119, Украина

ГОСУДАРСТВЕННО-ЧАСТНОЕ ПАРТНЕРСТВО В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ КАК ВАЖНЫЙ ФАКТОР ЕВРОПЕЙСКОЙ СТАБИЛЬНОСТИ

Резюме

Статья посвящена анализу преимуществ государственно-частного партнерства в сфере кибербезопасности. Информационные технологии играют доминирующую роль в развитии современного общества. Прогресс в этой области связан с появлением более сложных угроз. Система информационной безопасности является одним из «столпов» международной стабильности. Появилась необходимость выделить кибербезопасность как составляющую общественной жизни. Государство должно играть особенно важную роль в системе информационной и кибербезопасности, поскольку оно может принять ряд организационных и технических мер по защите своего информационного пространства. В статье отмечается, что добиться успеха можно лишь привлекая частный сектор. В мире существует много примеров эффективного государственно-частного партнерства (ГЧП).

Общей целью участия в ГЧП как для частного сектора, так и для государственного, является повышение кибербезопасности. Однако существует ряд различных причин, почему партнерство может быть полезным для государственных и частных структур и какими могут быть общие выгоды от ГЧП. Например, для государственных структур причинами могут быть: ограниченность инструментов реализации государственной стратегии; отсутствие средств для привлечения всех малых стейкхолдеров к защите критической инфраструктуры; системное понимание критической инфраструктуры для защиты информации; возможность создания эффективной связи между различными инициативами частного сектора; доступ к ресурсам частного сектора (например, к экспертам), что облегчает установление стандартов. Для частных компаний причинами могут быть: решение проблемы за пределами организационных возможностей компании; недостаток вовлеченности высших руководителей в действия; возможность влиять на будущую стратегию национальной безопасности; заинтересованность в действенных механизмах нейтрализации неадекватного государственного регулирования; доступ к государственным средствам; возможность влиять на национальное законодательство и обязательные стандарты; уверенность в качестве продуктов и услуг, поставляемых через ГЧП, поскольку это

гарантируется правительством. Для общей выгоды причинами сотрудничества могут быть: желание устранить уязвимость от ранее пережитого негативного опыта; наличие провалов в обеспечении этапов цикла безопасности; развитие угроз с национального уровня на международный; недостаток доверия между конкурентами в пределах географических, секторальных или тематических областей, а следовательно, потребность в создании надежной структуры для решения этой проблемы; обмен знаниями, опытом; достижение устойчивости киберсистемы. В статье доказывается, что существует потребность совместить возможности, потенциал государственного и частного секторов для борьбы с киберугрозами. Каждая страна пытается найти свой путь в построении ГЧП. Надежный сектор кибербезопасности помогает не только защитить государство и его граждан, но и стать двигателем экономического роста. Особенно активными и успешными в сфере ГЧП являются страны-члены ЕС. Статья исследует особенности государственно-частного партнерства в сфере кибербезопасности в ЕС.

Ключевые слова: государственно-частное партнерство, кибербезопасность, международная безопасность, ЕС.