PUBLIC-PRIVATE PARTNERSHIP IN CYBERSECURITY: INTERNATIONAL EXPERIENCE AND OPPORTUNITIES FOR UKRAINE

Analytical report

(abridged version)

Authors:
D. Dubov, Doctor of Political Sciences, Senior Research Fellow – Foreword, Chapter 1, Par. 4.4., 4.5.
V. Boiko, Candidate of Historical Sciences – Par. 3.1. and 3.2.
S. Hnatyuk, Candidate of Historical Sciences – Par. 4.1., 4.2. and 4.3.
T. Isakova – Chapter 2
M. Ozhevan – Doctor of Philosophical Sciences, Professor – Par. 3.4.
A. Pokrovska – Par. 3.3.

English translation – **A. Pokrovska**

Public-private partnership in cybersecurity: international experience and opportunities for Ukraine : analytical report / D. Dubov, V. Boiko, S. Hnatyuk, T. Isakova, M. Ozhevan, A. Pokrovska; General editorship of D. Dubov. – Kyiv: The National Institute for Strategic Studies, 2018 – 84 p.
ISBN 978–966–554–296–7

This analytical report considers the issues of establishing an effective public-private partnership in cybersecurity. The theoretical approaches to public-private partnership and their peculiarities in the cybersecurity sphere are analyzed. The international experience (the USA, the EU, Germany, the United Kingdom, and Poland) in building trust between the public and private sectors in the area of cyberspace security is researched. The legal and institutional frameworks of public-private partnership in Ukraine are considered, effective examples of such partnership are presented. Promising directions of developing cybersecurity public-private partnership in Ukraine and possible ways to implement them are outlined.

DETAILED CONTENTS

INTRODUCTION

Nowadays, public-private partnership (hereinafter, PPP) is recognized both by state and non-state actors as a key element in building a truly effective cybersecurity system of the state. Almost every cybersecurity strategy (of national or supranational level) or a departmental vision document (which deals with cybersecurity) mentions the desire to develop PPP.

At the same time, despite such unity of views, the practice of implementing cybersecurity PPP (hereinafter, CPPP) is still highly ambiguous and controversial (for example, although the International Telecommunication Union's "Global Cybersecurity Index 2017" rating contains the column "public-private partnership", it is measured quite carefully – in green, yellow and red colors, without providing meaningful measurement methodology[1]).

The given study is an attempt to start a broader discussion on this issue in Ukraine, covering, on the one hand, the already existing experience of particular Western states in the field of PPP development, and, on the other, key Ukrainian problems in the context of CPPP creation. The study results in recommendations that we believe will help both public authorities and non-state actors (primarily business, but also NGOs and scientists/experts) to better understand the possible ways to solve the problem of developing CPPP in Ukraine.

The first chapter of the report covers the general theoretical approaches to PPP as such and to the understanding of the very possibility of implementing CPPP.

The second and third chapters of the paper describe the problems of developing CPPP in economically and technologically advanced states that have a significant history of the formation of CPPP mechanisms and actually have powerful business actors to build up such relations, or those countries that have just started creating CPPP, but are doing this within the European regulatory space. Therefore, the USA, the United Kingdom, Germany, and Poland were selected for the analysis.

The fourth chapter focuses entirely on the problems in this area in Ukraine, where the situation is further complicated by many specific circumstances inherent mostly in our country. Primarily these are:

- the ambiguous legal framework that regulates CPPP (including on the issue of hacktivist activity);
- a number of issues (in particular, in implementing cybersecurity standards), which are mostly solved in the Western states;

[1] Global Cybersecurity Index 2017 [Електронний ресурс]. – Режим доступу : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

- a significantly higher activity of the civic sector, which strives to take a greater part in ensuring cybersecurity of the state (especially after 2014, when a significant number of hacktivist groups emerged).

All this is complemented by more traditional problems such as, on the one hand, the excessive secrecy of security structures and the visible trend towards ever-increasing control, on the other – often overestimated expectations and "maximalism" from the private and non-governmental sectors that are not always able to develop a constructive agenda for discussion with the state, do not have the proper knowledge of the real possibilities and limitations of state institutions in this sphere, are often poorly aware of the peculiarities of Ukrainian legislation, and are clearly lacking in unity of views on what CPPP should and can be at all.

The authors of the report did not aim to provide comprehensive answers to all questions in this area but tried to generalize the international experience in establishing CPPP, to understand the objective limits of CPPP and to identify the key problems associated with developing CPPP in Ukraine. As a result of this review some recommendations are suggested; to the authors' conviction, they will allow making the dialogue between public and private actors on CPPP more productive and giving it particular institutional forms.

The abridged version of this report contains only the introductory part, conclusions and key recommendations developed by the team of authors. Full content is available in Ukrainian (http://en.niss.gov.ua/)

CONCLUSIONS

1. CPPP remains an extremely complex and ambiguous phenomenon, which is formed within the conditions of mutual distrust of its participants and the lack of methodological approaches to understanding the very nature of PPP in this domain. Although most of the developed countries have some working forms of CPPP, almost in every case they are formed in ad hoc regime and under the significant influence of the historical experience of each particular country. Moreover, it can be noticed that virtually no country today has been able to create a CPPP system, which could be called exemplary and which would completely solve all the key issues arising in the cybersecurity sphere.

2. At the all-European level, the process of visioning in the CPPP domain is still mostly observed, although key strategic documents on cybersecurity include the PPP component. In particular, the European Commission initiated an Action Plan based on the Digital Single Market Strategy of 2015, the EU Cybersecurity Strategy of 2013 and the EU Directive on Security of Network and Information Systems to be implemented in the national legislation of the EU member states until May 9, 2018 and in internal statutory documents of the main enterprises till November 9, 2018.

3. While searching for effective forms of CPPP the European Commission held consultations with large, small and medium-sized businesses, associations, research institutions, the civic sector, public and regional authorities. Consultations lasted for 12 weeks. Obviously, the EC's consultation mechanism should become the basis for the respective process Ukraine needs.

4. Despite that CPPP is generally beneficial for both sectors, private companies are still cautious about its implementation. One of the key remaining problems here are trust, control, and disclosure of corporate information.

5. Almost all analyzed countries had a clear emphasis on the development of CPPP in only one or two aspects, although at the legal level (primarily in strategic documents on ensuring cybersecurity) CPPP was described as a basic element that needs comprehensive development for all its components.

6. In particular, for the USA, one of the main areas of CPPP is the mutual exchange of information on cyberthreats between the government and the private sector, which are embodied in legislative and institutional initiatives. At the same time, such cooperation revealed both the advantages and disadvantages of CPPP. On the one hand, CPPP helped investigate criminal and civil crimes, prevent cyberattacks, and create new methods for preventing and countering cyberthreats. On the other hand, this interaction increasingly raises concern of representatives of private companies due to unidirectional information exchange, excessively closed nature of state bodies, which raises the question of the viability of such cooperation.

7. In Germany, CPPP is aimed primarily at establishing mutually beneficial rules for the operators of critical infrastructure. At the current stage, despite the large number of mechanisms created for the purpose of implementing CPPP, the relevant system in Germany is still at the stage of formation, and a significant number of issues (particularly in CPPP regarding objects of critical infrastructure) is objectively unresolved.

8. The search for cooperation mechanisms is conducted within the framework of *UP KRITIS*, the main task of which is to prepare and implement joint recommendations for the state and private sector in cyberdefense. *UP KRITIS* regularly informs its participants and partner organizations from other countries about relevant European measures to protect critical infrastructure. Decisions taken by *UP KRITIS* members are presented for consideration by European structures, influencing the European agenda at the early stages, strengthening Germany's interests in this security sector. There also exist other cooperation platforms that have mixed public-private funding, such as the Cybersecurity Alliance – an initiative of the federal government of Germany, in which key players, both public and private, exchange information, create and expand the database to enhance cybersecurity in Germany.

9. For their part, German government structures (guided by the National Cyber Defense Strategy of 2011) also take measures that can be qualified as CPPP. In particular, the Federal Office for Information Security (*BSI*) has several structures (including the National Cyber Response Centre) aimed at providing better coordination in countering cyberattacks and more operational exchange of information between the government and the private sector. The given Center establishes conditions for all competent authorities to respond promptly to serious incidents, as well as analyzes and assesses threats, coordinates cooperation with local and sectoral organizations in crisis management.

10. CPPP in the United Kingdom at the current stage is focused more on searching purely market-based forms of interaction and on measures to enhance mutual trust. In particular, CPPP is developing within the framework of the public procurement mechanism and also plays an important role in providing state structures with high-quality services, specifically in the field of digital technologies. This is facilitated by the fact that the UK cybersecurity market is developing very dynamically, and to ensure its protection and sustainable functioning, the state and the private sector should bear enhanced joint responsibility, even if the essential goals of the state and business are different (the main thing for the state is citizen security, for business it is gaining profit).

11. The role of the British government in cybersecurity issues is not limited to total control and surveillance but lies in stimulating the private sector to cooperation, assisting innovation startups, coordinating cybersecurity tools, and supporting networks of cybersecurity experts. Despite the state's commitment to developing the partnership, business does not always voluntarily warn state

structures about the threats faced and possible to prevent, which stipulates the need for stricter regulation.

12. An excellent example of consolidating the efforts of the various UK cybersecurity authorities is the functioning of the National Cybersecurity Center (GCHQ component), which is guided in its practice by the principles of seeking understanding with business and involving state, business, science and civic representatives in the process of developing best practices, recommendations and guidelines for implementing high standards of cybersecurity, including sectoral ones.

13. According to the legal practice established in the Republic of Poland, the following should be attributed to the basic characteristics of CPPP: mutual benefit; civil law nature; a specific goal (the construction of infrastructure facilities, the provision of specific services, traditionally performed by the public sector, etc.); optimal division of tasks between the public and private sectors of cooperation; division of risks between the two sectors. The discussions in Poland around the essence of CPPP relate primarily to the possibility of its identification/distinction with concessions. There are two contrary positions: the identification of these forms of interaction between the public and private partners and their strict separation.

14. Today, Poland is mainly focused on the development of the CERTs system, actually by "embedding" separate forms of CPPP (including with the banking sector and the scientific community) into their activities (first of all, CERT NASK and NCC created on its basis). An important role in institutionalizing Poland's CPPP is played by government structures, primarily the Ministry of Digitization as well as by the regulatory framework identifying the need to implement CPPP.

15. As of fall 2017, the state adopted only basic framework acts for the establishment of the legal ground for CPPP in Ukraine – the Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine", as well as the Cybersecurity Strategy of Ukraine approved by the Decree of the President of Ukraine of 15 March, 2016, № 96/2016. At the current (initial) stage, they do not form an appropriate legal basis for launching sectoral CPPP as they are not backed by the relevant by-laws (including the registry of the National critical information infrastructure (NCII) and contain many controversial or abstractly formulated definitions, provisions, and norms. Namely:

- the legal content of the very concept of "public-private interaction" (PPI) remains unclear, particularly its correlation with the Law of Ukraine "On Public-Private Partnership" and other regulations;
- the mechanisms and procedures for the sectoral regulation of protecting cybersecurity objects are insufficiently articulated, the opportunities for PPI in this sphere are not considered (most notably, the introduction of non-state sectoral regulators, which proved to be effective in international practices);

- the procedure of implementing information security audits on NCII objects, setting requirements for information security auditors and determining the procedure for their certification require further harmonization based on the balance of powers and interests among all stakeholders;
- standardization of the institute of independent auditors on the same basis is also needed;
- the issues of standardization in cyberdefense and information security remain unresolved, primarily in terms of procedures and limits of the application of the relevant Ukrainian and/or international standards (especially critical for developing PPI with the participation of NCII objects).

16. Although both the non-state sector in Ukraine and state institutions sometimes show significant potential for establishing a nationwide CPPP system, along with this, as of fall 2017, only some of its elements are still forming in Ukraine, but the system itself yet does not exist.

17. Along with the imperfect legal framework, the second fundamental problem of developing PPI is the lack of articulated and effective state policy, primarily communicative and regulatory. In this context, it is becoming increasingly crucial for competent authorities to (a) establish proper communication/cooperation with the non-state sector (industry-specific business associations, professional nonprofit organizations, expert circles, etc.), and (b) establish effective institutional and legal instruments for such interaction.

18. Another remaining problem in developing an effective CPPP in Ukraine is that Ukraine's cybersecurity sector is extremely closed, and the available information about it does not give an objective picture of its condition and prospects. This necessitates the review of Ukraine's cybersecurity sector and drawing up a relevant document on its basis, which will allow forming a holistic view of problems in the cybersecurity sphere, evaluating resources for solving problems and outlining possible strategies for solving existing problems.

19. Political hacktivism becomes a significant factor in the general issues of cybersecurity in Ukraine. Engagement of volunteer and non-governmental organizations in countering Russian aggression by attacking computer systems of Russian-terrorist groupings, as well as computer systems on the territory of the Russian Federation, has indeed provided valuable assistance in countering Russian aggression and helped to publicize evidence of Russia's active engagement in the conflict in the East of Ukraine.

20. At the same time, attempts by Ukrainian hacktivists to partially reorient their activities from external platforms to domestic ones (resorting to unauthorized pen-tests of state systems) are mostly illegal under the current legislation and can be qualified by Art. 361 of the Criminal Code of Ukraine. Without a legal solution to this problem, an effective CPPP between the state and activist groups (individual cybersecurity experts) will be significantly complicated.

21. Given the often lack of even basic elements necessary for the establishment of an effective CPPP in Ukraine, the key practical steps in this domain are the following:

- drawing up a list of areas/objectives of CPPP (both for the state and private sector), impossible for them to reach without each other;
- defining (on the basis of broad discussion and high-quality scientific-expert research) criteria of CPPP as an attractive solution for both parties;
- implementation of systemic measures aimed at strengthening the CPPP participants' confidence in each other;
- assistance from non-governmental organizations and the scientific-expert community to both parties in defining the partnership goals and in developing long-term strategies for such a partnership;
- searching for effective approaches to identifying risks for each of the parties, as well as optimal forms of responsibility;
- development of discussions between the two partnership parties in order to solve existing problems and create permanent discussion platforms;
- discussion of possible joint projects (both on the basis of co-partnership and co-financing).

KEY RECOMMENDATIONS

1. Ukraine needs an open and wide-ranging debate on CPPP, the results of which could be embodied in a clear and comprehensible state strategy document (the "Strategy for Public-Private Partnership in Cybersecurity" or the "Concept of Public-Private Interaction in Cybersecurity"). This document should be drafted with the active involvement of stakeholders and, to a greater extent, be a product of the non-state sector, than the state structures.

2. To this end, it is proposed to create a basic "Cyberdialog" online platform (the product of the Initiative working group, which should include key non-state actors of the cybersecurity market (including system software integrators, antivirus software vendors), representatives of specialized IT associations, as well as representatives of scientific institutions) and which should form the basis for public consultations with stakeholders on the planning of the future strategy for public-private partnership in cybersecurity.

3. Through a consultation mechanism, a consensus view should be developed on a number of key issues that will further form the basis for the CPPP framework document: sectoral requirements for CPPP implementation; CPPP stakeholders (possibly in the form of a relevant draft register); risk assessment methodologies (based on international standards and practices); typical models of CPPP projects with the definition of legal, institutional, investment and other mechanisms for their implementation; the procedure for certification of auditors and conducting audits (with reference to the relevant legal acts); a mechanism for establishing continuous multilateral exchange of relevant information among all participants of CPPP; sources and mechanisms to stimulate CPPP; ways and mechanisms to support research and development (R&D), as well as preparation of draft concept documents in the cybersecurity sphere and within the CPPP framework; procedure for exercises, trainings, etc.

4. Following the consultations, the draft "Strategy for Public-Private Partnership in Cybersecurity" or the "Concept of Public-Private Interaction in Cybersecurity" should be prepared. It is reasonable to involve to the process of developing (consulting) the text the representatives of European structures that either have experience in working out relevant strategies or are currently engaged in the processes of reforming the security and defense sector of Ukraine such as: EUAM[2], the EC representatives who participated in the elaboration of the European public-private partnership on cybersecurity. It is expedient to approve this Strategy by the relevant decision of the NSDC of Ukraine within the framework of the Cybersecurity Strategy of Ukraine. It is also advisable to consider the possibility of holding by the National Coordination Center for Cybersecurity of at least one meeting per year devoted to the state of

[2] EUAM Ukraine [Електронний ресурс]. – Режим доступу : http://www.euam-ukraine.eu/ua/our-mission/our-priorities/

implementation of public-private partnership (possibly involving representatives of the non-state sector).

5. It is impossible to solve the CPPP problem without a more precise definition of the very concept of “public-private partnership” mentioned in the Cybersecurity Strategy of Ukraine, as well as “public-private interaction” referred to in the Law “On the Basic Principles of Ensuring Cybersecurity of Ukraine”.

6. It is important to work out the possibility of implementing Germany’s experience in Ukraine in the part of approval by the subjects of the national cybersecurity system, which are directly responsible for developing and monitoring compliance with standards in this sphere, for operators of critical infrastructure objects, of the cybersecurity industry standards to be proposed by operators themselves.

7. Moreover, Ukraine should insist on including the CPPP topic in programs implemented within the NATO-Ukraine Trust Fund on Cyber Defense while the Ministry of Foreign Affairs of Ukraine should engage the experience of international partners in the development of new CPPP mechanisms in the field of cyberdefense and exchange of information on cyberthreats.

8. The State Special Service of Special Communication and Information Protection together with representatives of the business environment (first of all, operators of critical infrastructure objects) should initiate the launch of the “Program on cooperation and cyberinformation exchange” (based on the principles of the similar American program *CISCP*). To more effectively implement such program, it is proposed to involve as consultants the experts from the US Department of Homeland Security who are responsible for the support and implementation of the *CISCP*.

9. It should be taken into account that the principles of protecting privacy and civil liberties should be an integral part in drafting and implementation of the “Program on cooperation and cyberinformation exchange”; these principles can be formed on the basis of common standards and guidelines such as the US *Fair Information Practice principles*.

10. It is advised to consider the possibility of introducing a secure online mechanism for the exchange of information on cybernetic threats between representatives of the cybersecurity industry and electronic communications, on the one hand, and the subjects of the national cybersecurity system, on the other, similar to British *CISP*. Such mechanism should be developed under the auspices of the National Coordination Center for Cybersecurity with the participation of experts from business, leading research institutions, state authorities and the civic sector.

11. Mechanisms for regular dialogue between private companies and the government (seminars, forums, training) should be involved to promote and

implement CPPP initiatives. One of the mechanisms for implementation can be the launch of an annual international/all-Ukrainian forum on public-private partnership in the cybersphere with the participation of key actors of the national cybersecurity system and non-state stakeholders.

12. Subjects of the national cybersecurity system together with representatives of the national information industry should form a pool of experts who can be involved in:

- investigating cyber incidents on critical infrastructure objects and addressing consequences;
- communicating incidents in the media;
- professional development programs for staff members of the national cybersecurity system and for critical infrastructure personnel;

The pool of experts can be formed by sectoral manner and reviewed annually.

13. During the process of forming the Action Plans for implementing the Cybersecurity Strategy of Ukraine it is necessary to take into account the need to expand the measures aimed at realizing public-private partnership. In particular, it is necessary to foresee the possibility of creating a Ukrainian analog of KRITIS, which should have the functions of:

- preparing the implementation of joint recommendations for the public and private sector in cybersecurity;
- conducting trainings for CPPP parties;
- interaction with international partners and similar structures;
- crisis communication;
- informing national partners about relevant European structures on the protection of critical infrastructure;
- setting up the procedure of adding participants to this platform.

14. The Cabinet of Ministers of Ukraine should make more efforts to resolve the issue of launching a wide-ranging expert and public discussion on establishing a platform for public-private partnership in cybersecurity, while ensuring due publicity and media support for such discussion: online platform (s), web-broadcasts, preparation of relevant TV programs and other forms of TV-promotion. The results of the discussion should be presented to the public.

15. It is important to initiate discussions on the modification of Ukrainian legislation (including the Criminal Code of Ukraine, first of all, Article 361) to legalize pen-tests by hacktivists (“white hacking”) for checking the readiness of critical infrastructure objects to possible cyberattacks and cyber incidents.

16. It is advisable to work out a viable mechanism for coordinating the hacktivists’ actions with government structures, making it much less bureaucratic and guaranteeing non-disclosure of information on such cooperation. There are

two ways of solving this issue. The first is to form a permanent working group on special issues of public-private partnership under the National Coordination Center for Cybersecurity. The second is the working group within the authority responsible for covert inspection of the readiness of critical infrastructure objects to possible cyberattacks and cyber incidents (currently the SSU is responsible for this).

17. The Cabinet of Ministers of Ukraine and the Verkhovna Rada of Ukraine should consider the issue of launching a public-private coordination platform with advisory powers (for example, in the form of a temporary commission or committee) to participate in drafting legal acts on the independent audit of information security at NCII objects on the basis of international standards, including the European Union and NATO.

18. It is also important for the subjects of Ukraine's national cybersecurity system to initiate consultations on establishing an open online platform for sharing cybersecurity experience between the state, science, business and the civic sector, analogous to the British *Cyber Growth Partnership* initiative. Actual creation of an online platform is possible, in particular, through private and volunteer efforts.

19. To learn from the private sector's practical experience in preventing cyberthreats, responding to cyber incidents and protecting the information systems of key subjects of the national cybersecurity system, it is expedient to develop a mechanism for involving proven private-sector experts to work on projects within the units responsible for cybersecurity at government agencies. The remuneration of such specialists is possible through projects of international technical assistance, as well as, if possible, with funds allocated within the framework of the NATO-Ukraine Trust Fund on Cyber Defense.

20. For broader scientific and information support of the subjects of the national cybersecurity system it is recommended to establish cybersecurity centers of excellence at key higher educational institutions of Ukraine. It is relevant to open pilot centers at the leading educational institutions such as the Educational and Scientific Institute of Information Security at the SSU Academy, the Institute of Special Communications and Information Protection at NTUU KPI, the Military Institute of Telecommunications and Informatization, Taras Shevchenko National University of Kyiv, State University of Telecommunications.

21. The State Service of Special Communications and Information Protection of Ukraine and other subjects of the national cybersecurity system should consider the institutional, resource and legal framework for further expansion of CPPP with industry associations and other non-state actors in the exchange of information on cyber incidents, expert and technical cooperation, in preventing and investigating cyberattacks (in the context of launching a nationwide data exchange system on cyber incidents).

22. It is essential to raise awareness of citizens in the cybersecurity sphere and to ensure the appropriate level of computer literacy among institutions, companies, and enterprises. Therefore, the Ministry of Education and Science of Ukraine should endeavor to establish systemic cooperation with specialized non-governmental organizations for the joint development of specialized curricula for higher and secondary schools, participation in the educational process based on the concept of continuing education – postgraduate, distance, informal (training, courses) education, optional programs for students of non-core universities and schoolchildren, etc.

23. As a major pilot CPPP project, a “Cybersecurity Survey” could be prepared with the involvement of all stakeholders; the survey should describe the current state of Ukraine’s cybersecurity sphere, its resource potential, and ways to optimize the cybersecurity capabilities. One of the formats of this review may be the use of existing procedures for integrated cybersecurity assessments. In particular, it is relevant to more effectively study the experience of such surveys by international cybersecurity organizations (specifically the *Business Software Alliance*), and the Review itself can be structured by the following scheme:

- the legal basis for the functioning of a particular piece of cyberspace;
- organizational institutions and mechanisms for ensuring cybersecurity;
- the state of public-private partnership;
- sectoral cybersecurity;
- cybersecurity education.