УДК 346.22
DOI https://doi.org/10.24144/2788-6018.2024.06.57

PUBLIC-PRIVATE PARTNERSHIP IN THE FIELD OF CYBERSECURITY

Sieriebriak S.V.,
Doctor of Law, Associate Professor of the
Department of Public and Private Law
Volodymyr Dahl East Ukrainian National University
ORCID: 0000-0001-7207-594X

Sieriebriak S.V. Public-private partnership in the field of cybersecurity.

The article provides a comprehensive analysis of the legal framework for public-private partnership relations in Ukraine. The author considers the main conceptual approaches to understanding the concept of "public-private partnership", which allows clarifying its legal nature as a form of cooperation between public authorities and private entities to solve socially important tasks. Particular attention is paid to the historical and legal grounds for the emergence of public-private partnership, which is the result of a long process of evolution of relations between the State and private entities in the context of jointly addressing key socio-economic issues.

The author identifies a number of problematic aspects which complicate the effective implementation of public-private partnership mechanisms in economic relations in Ukraine. In particular, these include imperfections in the legal framework, insufficient transparency of the procedures for concluding public-private partnership agreements, limited financial resources and low level of trust between public authorities and private partners. The article proposes ways to improve domestic legislation, in particular, to clarify the procedural support for the implementation of public-private partnership projects, increase transparency, and introduce clear mechanisms for monitoring the fulfillment of the terms of such agreements. The author analyzes in detail the peculiarities of legal regulation of public-private partnership in the field of cybersecurity in Ukraine. It is shown that domestic practice is still at the stage of formation, which requires the introduction of a systematic approach to the development and implementation of relevant projects. The relevance of this area in the context of ensuring Ukraine's cybersecurity and integration into the European and international cyber defense system is determined.

Specific recommendations for improving current legislation are proposed, in particular, to strengthen legal guarantees for partnership participants, develop mechanisms to encourage the private sector to participate in public-private partnership projects in the field of cybersecurity, and implement best practices in cyber risk management.

Thus, the article not only summarizes the current state of development of public-private partnerships in Ukraine, but also identifies priorities for its improvement, especially in the field of cybersecurity, which is a key component of national security in the face of current challenges.

Key words: public-private partnership, legal support, economic relations, digitalization, information and communication technologies, cyber defense.

Сєребряк С.В. Державно-приватне партнерство у сфері забезпечення кібербезпеки.

У статті здійснено комплексний аналіз правового забезпечення відносин у сфері державно-приватного партнерства в Україні. Розглянуто основні концептуальні підходи до розуміння поняття «державно-приватне партнерство», що дозволяє уточнити його правову природу як форми співпраці державних органів та приватних суб'єктів для вирішення суспільно важливих завдань. Особливу увагу приділено історико-правовим підставам виникнення державно-приватного партнерства, яке є результатом тривалого процесу еволюції відносин між державою та приватними структурами в контексті спільного вирішення ключових соціально-економічних проблем.

Виділено низку проблемних аспектів, що ускладнюють ефективне впровадження механізмів державно-приватного партнерства у господарські відносини в Україні: недосконалість нормативно-правової бази, недостатній рівень прозорості процедур укладення договорів державно-приватного партнерства, обмеженість фінансових ресурсів та низький рівень довіри між державними органами і приватними партнерами.

Детально проаналізовано особливості правового регулювання державно-приватного партнерства у сфері кібербезпеки в Україні. Показано, що вітчизняна практика поки що перебуває

на етапі становлення, що потребує запровадження системного підходу до розробки та реалізації відповідних проєктів. Визначено актуальність даного напряму в контексті забезпечення кібербезпеки України та інтеграції до європейської та міжнародної системи кіберзахисту.

Запропоновано конкретні рекомендації для удосконалення чинного законодавства, зокрема стосовно посилення правових гарантій учасників партнерства, розробки механізмів стимулювання приватного сектора до участі в проєктах державно-приватного партнерства у сфері кібербезпеки та впровадження передових практик управління кіберризиками.

Таким чином, стаття не лише узагальнює поточний стан розвитку державно-приватного партнерства в Україні, а й визначає пріоритети для його вдосконалення, особливо у сфері кібербезпеки, яка є ключовою складовою національної безпеки в умовах сучасних викликів.

Ключові слова: державно-приватне партнерство, правове забезпечення, господарські відносини, цифровізація, інформаційно-комунікаційні технології, кіберзахист.

Problem statement. As in all other countries oriented to a democratic model of development, only a part of the national critical information infrastructure in Ukraine is under direct control of the state (in terms of ownership and administrative and legal influence). A significant segment of it – in the energy, chemical, transportation, ICT, banking, utilities, etc. sectors - is privately owned and otherwise controlled. At the same time, both Ukrainian and international experience shows that:

1) non-state cybersecurity facilities are usually the most vulnerable to cyberattacks;

2) full protection of such facilities requires joint efforts of the private and public sectors and systematic interaction between them;

3) broad public-private partnerships in the field of cybersecurity, not limited to national critical information infrastructure, are mutually beneficial and contribute to the optimization of sectoral state policy and strengthening of national security (subject to adequate institutional and legal regulation, of course).

The aim of the study. The purpose of this article is to define the basic principles of legal regulation of public-private partnership in the field of cybersecurity, and to propose proposals for developing effective mechanisms of legal regulation.

State of the art of the issue. The challenges of our time, such as international aggression, terrorism and the spread of economic crises, make it clear that ensuring national security is a matter not only for the state, but also for every citizen. Joint problem-solving with the private sector in the field of security and defense of Ukraine, attraction of private investments in the implementation of state projects, attraction of private innovations, improvement of the scientific and technical base of the public sector, fulfillment of state defense orders by non-governmental organizations - all this gave impetus to the development and scientific substantiation of public-private partnership in the defense industry of Ukraine.

Certain aspects of public-private partnership both in general and in the security sector of Ukraine have been the subject of scientific research in the works of Markieieva O.D., Rozvadovsky B.L., Mashchenko M.A., Simak S.V., Petrova I.P., Sirant M.M., Kruglov V.V. and others. However, there is still no effective mechanism for ensuring cooperation between the state and the private sector at both the international and national levels, although certain steps are being taken.

Summary of the main material. The critical need to expand public-private partnerships in the field of cybersecurity in today's globalized society is explained by a set of objective factors. Experts identify several primary reasons for strengthening cooperation between government agencies and the private sector:

1) the deepening privatization process in various segments of critical infrastructure, which is observed both in Ukraine and internationally, leads to a situation where state institutions are unable to provide comprehensive protection of key information assets on their own;

2) intensive accumulation and dissemination of electronic data that are of strategic importance for the smooth operation of both private companies and government agencies;

3) the growing dependence of national and international infrastructures on information and telecommunication networks, which are highly vulnerable to cyber threats;

4) increased interconnectedness and integration of computer systems, which creates risks of chain reactions: damage to one network may adversely affect the functioning of other infrastructure elements;

5) limited financial and technical resources of small and medium-sized enterprises, which cannot provide an adequate level of cyber protection on their own and therefore need support either from government agencies or large corporations capable of providing appropriate information resources protection services.

Thus, building a partnership between the state and the private sector in the field of cybersecurity is becoming not just a desirable but an extremely necessary step to reduce cyber risks and ensure the resilience of information infrastructure at the national and global levels.

That is why various forms of public-private partnerships in the field of cybersecurity are now considered one of the main tools for building effective cybersecurity systems and are widely used in international practice. Ideally, this allows them to be combined in the formation of a national cybersecurity system.

The historical trend towards greater participation of the private sector in the life of the state emerged in the late 70s of the twentieth century in Western countries, which was associated with the global economic crisis of that time [1].

Neoliberal theory suggests that one of the effective methods of overcoming the existing crisis is to radically reduce bureaucracy and transfer certain state powers to private actors, or at least to introduce models of partnerships between the public and private sectors. The first public-private partnership projects were mainly aimed at developing urban infrastructure, implementing environmental programs, as well as healthcare and education. Later, with the expansion of the range of industries to which the public-private partnership mechanism is applied, some researchers began to point out that the essence of this concept may be blurred. Public-private partnership is increasingly being used as a universal term to refer to a variety of new or little-known forms of interaction between the state and private entities, which, according to some experts, leads to the loss of a clear meaningful meaning of this legal institution [2].

Currently, in Ukraine, as well as in the EU member states, public-private partnership is the highest form of interaction (cooperation) between the state and society, characterized by the attraction and exchange of resources provided by the non-governmental sector in order to increase innovation and efficiency in the public sector, as well as the development of certain areas.

Turning to the issue of models of public-private partnership in the security sector of Ukraine, it should be noted that public-private partnership in the security and defense sector of Ukraine is not provided for at the legislative level. According to the Law of Ukraine "On Public-Private Partnerships", public-private partnerships can be implemented in the following areas of the most important public life: production, transportation and supply of natural gas; construction and/or operation of roads, railways, bridges, ports; healthcare; mechanical engineering; water collection, treatment and distribution; tourism, recreation, recreation, culture and sports and others (Article 4) [3].

That is, only in areas that promote the public interest. Considering the provisions of Part 2 of the said Article, which indicates that by the decision of the state partner, public-private partnerships may be implemented in other areas of activity, except for those that are allowed to be carried out exclusively by state-owned enterprises [4], public-private partnerships can also function effectively in other areas that fall within the category of "public interest". An analysis of the legal doctrine [5, p. 107-108; 6, p. 63-64], current legislation of Ukraine, and the practice of the Supreme Court makes it possible to specify that:

1) the public interest is a certain set of private interests recognized by the State or its authorized administrative-territorial unit;

2) the public interest includes the interest of social communities, groups and society;

3) the category of "public interest" includes the state interest, the interest of adjacent territorial communities, the interest of a territorial community and public interests;

4) the subject of public interest is the good that is necessary for the full functioning of society.

The Law of Ukraine "On the Basic Principles of Ensuring Cybersecurity of Ukraine" not only enshrines public-private interaction and cooperation with civil society in the field of cybersecurity as one of the principles of cybersecurity in Ukraine, but also provides a list of ways to ensure public-private interaction: a) involvement of volunteer organizations; b) exchange of information between government agencies and the private sector; c) involvement of the private sector in the development of regulations; d) public control, etc. Similar provisions are enshrined in the Law of Ukraine "On Critical Infrastructure" [8].

The foregoing gives grounds to conclude that a) state security is a benefit that is necessary for the proper functioning of society and each individual; 2) the sphere of security and defense of the state contributes to the public interest, which necessitates proper interaction between the private and public sectors and the implementation of public-private partnerships; 3) the security sphere, within which public-private partnerships are implemented, is a rather broad concept, and includes cybersecurity, public safety, protection of critical infrastructure etc.

An important feature of public-private partnership in the security sector of Ukraine is the types (models) of its implementation. In general, the world practice includes many classifications of public-private partnership models. For example, in the United States of America, a set of public-private partnership models is quite common, which are divided, depending on the purpose of functioning, into: 1) partnerships that implement priority projects in the field of infrastructure (tender procedure); 2) partnerships that provide expertise to a private partner (for the implementation of large programs); 3) partnerships aimed at attracting new technologies; 4) partnerships aimed

at attracting financial resources; 5) partnerships aimed at managing public-private partnerships [9].

The introduction of public-private partnership mechanisms in the field of state security, an area in which the state has traditionally maintained its monopoly role, is particularly controversial. However, such a monopoly has never been absolute: at different stages of historical development, precedents of specific forms of public-private cooperation in the field of national security can be traced. This phenomenon was especially noticeable in the context of naval operations, when privateers were granted "privateer certificates" to conduct combat operations under the state flag. The modern analog of this practice is reflected in the activities of private military companies, which today occupy an increasingly significant niche in the security system, including the performance of various security and military tasks in conflict zones.

From a theoretical point of view, one of the most difficult issues arising from the expansion of public-private partnerships is the definition of criteria that allow for a clear distinction between a "true" public-private partnership and other forms of cooperation between the state and the private sector. The concept of public-private partnerships is based on two key principles that define the necessary conditions for its creation: neither party to the partnership can achieve a certain goal on its own without the participation of the other party; the partnership is based on a financial agreement that makes cooperation mutually beneficial for both parties.

These conditions provide the structural basis for public-private partnerships as a form of integration of resources and competencies of the state and the private sector to solve socially important problems. Stephen Linder characterizes it as follows: "the purpose of public-private partnerships is to exploit synergies in the joint innovative use of resources and application of management knowledge to optimally achieve the goals of all parties involved, if these goals could not be achieved without the involvement of these parties" [10].

In addition, he rightly notes that in the framework of public-private partnerships, both parties must change the nature of their thinking to ensure the success of the partnership - public-private partnership entities are forced to think and act like their partners, i.e., public participants must think and act like entrepreneurs, including how business must consider the public interest, and expect to be more accountable to the public [11].

At the same time, the cybersecurity sphere has certain unique problems that are still poorly understood and do not have universal "recipes" for solutions (moreover, they may not exist at all). The American researcher M. Carr draws attention [12] to the fact that even in the United States, where public-private partnerships have been defined as the cornerstone of the national cybersecurity system for almost 15 years, the parties have not been able to determine the parameters, nature and scope of such cooperation (moreover, the US Government Accountability Office report "Report on Critical Infrastructure Protection: Current Cyber Sector Specific Planning Approach Needs Reassessment" (2009) revealed a significant number of problems in the efforts of the US government to create a public-private partnership in the field of cybersecurity).

The effectiveness of public-private partnerships in the field of cybersecurity is largely related to how cybersecurity is defined in general and to what extent state cybersecurity and individual cybersecurity are correlated. In many cases, the rule "what is good for the security of the state is good for the security of the individual" does not work, and this is especially true in cybersecurity issues. In addition, there is almost always a lack of coordination in these relationships, which affects the very nature of PPPs. In this regard, Larry Clinton [13] aptly notes that "a partnership between citizens, or business, or government, can be much more complicated than expected. Lack of coordination about the roles of the partners, their responsibilities and expectations can lead to problems, even if the partners seem to have common goals. Communicating potential differences can also be problematic, even if the partners are sincere in their desire to succeed." Therefore, in his opinion, for effective public-private partnerships, the rational and meaningful management of these relationships may be even more important than the nature of these relationships (or their coverage of the entire set of cybersecurity areas).

An important component of strengthening the state's cybersecurity capabilities is the establishment of a constructive dialogue in the format of public-private partnership. The international experience gained convincingly proves that it is impossible to build effective and reliable cyber defense without comprehensive interaction between the state and the private sector. Public-private partnerships involve a form of cooperation that achieves goals and objectives that will contribute to national security, economic development and the construction of a secure cyber environment for all citizens. In other words, the public-private partnership model can be described as a dynamic interaction between public and private institutions that jointly perform functions to ensure security in cyberspace.

The experience of the United States in this area is interesting. A positive example of modern models of parity interaction between the public and private sectors in the field of cybersecurity is the creation of an automated cyber threat tracking program based on the US Department of Homeland Security, which allows for automated information exchange between the public and private sectors. Similar examples exist in European countries (the UK, the Netherlands). Also, in the United States, a non-profit research center "TechAmerica Foundation" was created to provide forecast support for the activities of government agencies and the private sector in the field of cybersecurity, which brings together specialists and experts from 1200 companies to determine the estimated annual funding for cyber defense, with the focus of activities constantly providing for a significant increase in spending based on potential and real cyber threats.

Also in the United States, a non-profit organization successfully operates as a private institute "SANS" (SysAdmin, Audit, Network and Security) [14], which is engaged in research, training and certification in the field of computer security. Today, SANS is one of the largest certification centers in this field, where, in addition to traditional training, experimental activities are carried out. In order to increase the audience of students, various formats are used - online training, scientific and practical events, conferences, etc. Every year, 12 thousand people around the world take a course at SANS. From time to time, this institution organizes competitions between its instructors and searches for new trainers.

Ukraine demonstrates positive experience in public-private partnerships in cybersecurity. Both the non-governmental sector in Ukraine and government agencies demonstrate significant potential for the formation of a full-fledged public-private partnership platform in the field of cybersecurity on a national scale. For example, it is on the basis of public-private partnership that work is underway to create a powerful cybersecurity center in Ukraine on the basis of the State Concern "Ukroboronprom". In addition to representatives of the National Security and Defense Council, the Ministry of Defense, the Security Service of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Cyber Police Department, NATO experts, consultants from the Turkish state-owned company HAVELSAN and specialists from NTUU "KPI", the project involves the non-profit organization "Ukrainian Academy of Cybersecurity" [15] and the Ukrainian team of "white" hackers DCUA (one of the strongest in the world) [16] . The Cyber Guard project of the state concern Ukroboronprom was implemented in partnership with private companies to protect private and public institutions of Ukraine from cyberattacks [17].

Conclusions. Thus, based on the generalization of the achievements of foreign experience of public-private partnership in the field of cybersecurity, the following components can be distinguished: its main goal is to build a constructive dialogue and fruitful cooperation, real trust between the private sector and public institutions; encouraging cooperation between public and private organizations in the early stages of the research and innovation process. Public-private investments are actively channeled into research programs to develop tools and prototypes to strengthen cyber defense and its components. Promising joint activities in the field of cybersecurity include: engaging startups and scientists to conduct computer and technical expertise; developing and implementing modern software to detect and prevent cyber threats at early stages; continuous monitoring of cyberspace; training of industry specialists, development and promotion of online educational platforms, etc.

REFERENCES:

1. Cavelty Myriam Dunn, Suter Manuel. Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*. December, 2009. Vol. 2, Is. 4. P. 179–187.
2. Linder S. Coming to terms with the Public-Private Partnership – A grammar of multiple meanings. Public-Private Policy Partnerships / P. Vaillancourt Rosenau (Ed.). The MIT Press, Cambridge MA, 2000. P. 19–36.
3. On public-private partnership: Law of Ukraine of 01.07.2010 № 2404-VI. URL: https://zakon.rada.gov.ua/laws/show/2404-17#Text. URL: https://zakon.rada.gov.ua/laws/show/2404-17#Text.
4. Chernadchuk V.D. The state and prospects of development of budgetary relations in Ukraine: monograph. Sumy: University book, 2008. 456 c.
5. Legal regulation of public revenues. Bulletin of Taras Shevchenko National University of Kyiv. *Legal Sciences*. 2005. № 64-65. C. 71–73.
6. On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine of 05.10.2017 No. 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
7. On Critical Infrastructure: Law of Ukraine of 16.11.2021 No. 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

8. Simak S.V. World experience in organizing public-private partnerships. Scientific works. Scientific and methodical journal. Petro Mohyla Black Sea State University. Series "Public Administration". Issue 223/201. Volume 235. C. 88–94.
9. Linder S., Vaillancourt P. Rosenau, Mapping the terrain of the Public-Private Policy Partnership. Public-Private Policy.
10. Partnerships / P. Vaillancourt Rosenau (Ed.). The MIT Press, Cambridge, MA, 2000. P. 1–19.
11. Linder, S.H. Coming to Terms with the Public-Private Partnership: A Grammar of Multiple Meanings. *American Behavioral Scientist*. 1999. № 43(1). P. 35–51. DOI: 10.1177/00027649921955146.
12. Madeline Carr. Public–private partnerships in national cyber-security strategies. URL: https://www.chathamhouse.org/sites/files/chathamhouse/ publications/ia/INTA92_1_03_Carr.pdf.
13. Clinton Larry. A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense. *Journal of Strategic Security*. 2011. Vol. 4, № 2. P. 97–112.
14. The SANS (SysAdmin, Audit, Network and Security). URL: https://www.sans.org/about.
15. Ukrainian Academy of Cyber Security. http://www.uacs.kiev.ua.
16. A single center for cybersecurity will be created in Ukraine with the support of NATO URL: https://goo.gl/4NL8TX.
17. Project of the state concern "Ukroboronprom" in partnership with private companies. URL: https://cyberguard.com.ua.