Public-Private Partnership in Cybersecurity

Vitalii Kruhlov [1][0000-0002-7228-8635], Mykola Latynin [2][0000-0002-7917-4518]
Alina Horban [2] [0000-0001-8866-4693] and Anton Petrov [3][0000-0003-3731-4276]

[1] Kharkiv National University of Civil Engineering and Architecture, Kharkiv, Ukraine
[2] Kharkiv Regional Institute of Public Administration of the National Academy for Public Administration under the President of Ukraine, Kharkiv, Ukraine
[3] National Aviation University, Kyiv, Ukraine
virt197@gmail.com, m.a.latynin@gmail.com
fartushnaya.alin@gmail.com

Abstract. The analysis of the possibility of providing cybersecurity through the use of public-private partnership (PPP) mechanisms is made. Public-private partnership is increasingly seen as addressing many of the challenges posed by cybersecurity management. Cybersecurity is intended to protect critical infrastructure and other important public functions against a variety of complex threats and is a central problem in today's security policy. In the process of implementing PPP cybersecurity, the state shifts the focus from control functions towards coordinating and motivating the fulfillment of security tasks by a private partner. Tasks to be addressed by public-private partnerships in cybersecurity are following: ensuring reliable access to the Internet; technical safety regulation; exchange of information on threats; assistance in resolving threat situations.

Keywords: cybersecurity, public-private partnership, projects, security policy.

CEUR-WS.org/Vol-2654/paper48.pdf

1 Introduction

One of the most difficult tasks that the state must address in today's context is the implementation of security functions. The development of the modern world, and above all its technological component, increase the likelihood of certain security risks. Critical infrastructure protection requires considerable measures and means. Changes that affect the development of both society and state have become increasingly unpredictable. The basic principles of the state's activity should guarantee the safe existence of a person, protection of his/her rights and freedoms, inviolability of life and private information. Security functions shape the sustainable activity of political life, socio-economic development, a favorable environment, secure information flows, and reliable infrastructure.

The modern activity of the state, economic entities, citizens, various associations is gradually lacking in full functioning without interaction with the sphere of information and communication technologies (ICT). The new phase of the industrial revolution, which is based on the intensive use of information and communication links,

Copyright © 2020 for this paper by its authors. Use permitted under Creative Commons License Attribution 4.0 International (CC BY 4.0). CybHyg-2019: International Workshop on Cyber Hygiene, Kyiv, Ukraine, November 30, 2019.

remote connections, processing and storage of information, requires the state to have a clear vision of threats and coordinated actions to implement security functions.

Existing network communications, server equipment, highly specialized professionals are in the field of private business, and therefore the issue of interaction with the state is important, given the role of ICT in the development of the economy, e-government, the operation of databases, exchange of confidential information, securing the work of strategic facilities and critical infrastructure. High priority of governments in most countries is placed on enhancing cybersecurity and ensuring the most vulnerable elements of infrastructure. The characteristic of system solutions in the field of information technology is a significant dependence on the private business entities that provide communication systems, computer networks, software development, create modern ICT equipment. This situation facilitates close cooperation between the state and the private sector within public-private partnership (PPP) models [1].

2 Data Protection in the Age of Industry 4.0

The issue of cybersecurity has become more pressing than ever, especially in the context of the combined efforts of manufacturers and users of information of different ownership forms. K. Schwab stressed the need for joint efforts of the state, business and civil society to maintain the security and reliability of government functions, communications and personal information stored and transmitted on digital platforms [2].

Data that show the influence of outsiders on information is growing in number every day. In the first half of 2018 alone, more than 4.5 billion records were broken [3]. Four new malwares are created every second. One of the most successful malware activities is phishing attacks, given that most phishing sites only last a few hours online. [4]. The number of network breaches in 2013-2018 (1st half year) in different directions is presented in Fig. 1.

Gartner reports that average annual security costs per employee have doubled: from $ 584 in 2012 to $ 1,178 in 2018. In some leading banks and technology companies, the total annual cybersecurity budget exceeds $ 500 million and continues to grow [5]. A report from the Center for Strategic and International Studies (CSIS) and McAfee notes that in 2017, cybercrime cost the world nearly $ 600 billion in spending, or 0.8% of global GDP, while in 2014, global losses amounted to about $ 500 billion dollars, or 0.7% of world GDP [6]. Given the rise in ICT users, the estimated cost of cybercrime by the end of 2019 could reach $ 2 trillion [7].

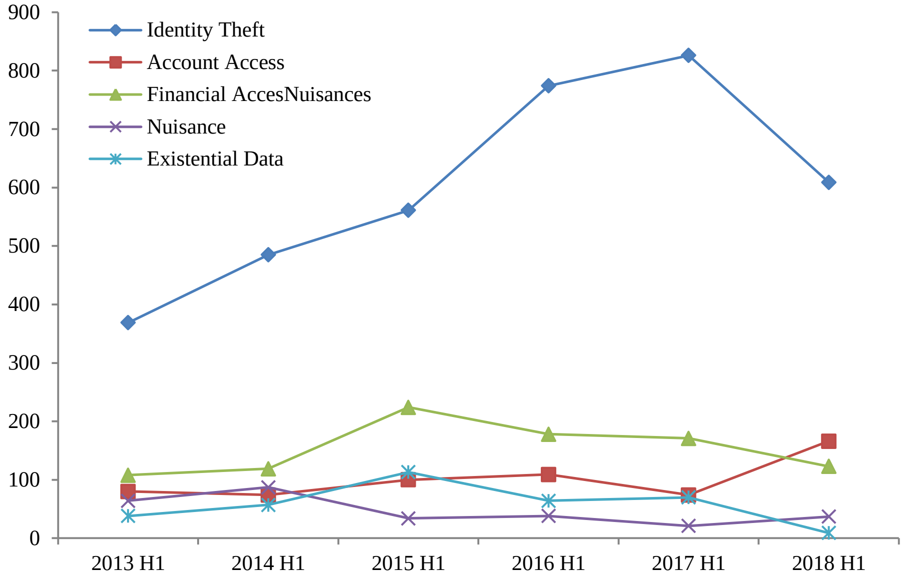

Fig. 1. Number of breach incidents by type over time (Source: [3])

Outdated digital infrastructure, lack of state-of-the-art technology solutions and software protections allow third parties to access restricted public information and control critical networks and financial accounts.

Using Artificial Intelligence by cybercriminals will create risks consisting of the following key cyber security issues:

- increasing the complexity of cyber attacks;
- action asymmetry - cyber attacks / protection;
- increasing in attack surface / digitization operation;
- balancing risks and operational capabilities [8].

The immersion of society and its dependence on information technology in various aspects of life has created a lot of spheres where crimes are possible [9]. The importance of ensuring the confidentiality of information, protecting national and public interests raises issues of implementing security policy by the state. Threats that have arisen in recent decades (cyberterrorism, cybercrime, information wars) are driving the state into partnering to execute its own functions to counter cybercrime.

The concept, called Industry 4.0, which was introduced in 2011 at the Hanover Industrial Exhibition in 2011, is another step on the way of manufacturing conversion based on the automation of production processes and information technology by the industry using the Internet of Things, global industrial networks, composite and volume printing production, artificial intelligence, virtual reality. The Fourth Industrial Revolution and emerging discoveries drive the development of new production technologies and business models that fundamentally transform global manufacturing systems [10].

It can be argued that the impact of new technologies related to artificial intelligence and robotics, the Internet of Things, virtual and augmented realities, blockchain technology and the new computer architecture is increasing every day. The proliferation of technology gives new opportunities for cybercrime and public and private sector representatives need to continue working together to mitigate new risks [11, p. 3].

The scale of developing and distributing programs that harm computer technology and steal personal data is steadily growing. In 2016 alone, 357 million new malware variants were released [12]. The WannaCry attack affected 300,000 computers in 150 countries, causing huge losses with Petya and NotPetya viruses. NotPetya alone caused the loss of about $ 300 million in the third quarter of 2017. The WannaCry attack has disrupted critical and strategic infrastructure around the world, including governments, railroads, banks, telecommunication providers, energy companies, automakers and hospitals [13].

According to A. Klimburg [14], cybersecurity has its special focus and lexis. Cybersecurity can be called a broad concept of security online, offline, and online [15]. Cybersecurity is implemented through actions to protect critical infrastructure and other important public functions against advanced persistent threat (APT) and other complex external attacks [16].

Cybersecurity is a key point in today's security policy, with cyber threats becoming the largest threats in the global threat assessment by the United States [17]. The UK Government is investing £ 1.9bn in line with the cybersecurity strategy put in force in 2017 with the official launch of the National Cyber Security Center [18]. Gradually, the understanding of a fully self-regulating and secure decentralized Internet is changing due to structural vulnerabilities that are not accessible to any individual entity [19]. These vulnerabilities are increasingly being used by criminals to provide services and malicious products for sale and widespread access, requiring multifaceted and coordinated approaches to enhance cybersecurity online. [20].

Thus, cybersecurity is provided at the physical infrastructure level within logical interfaces to run and connect infrastructures and levels of current content (information) on user-level networks (individual and corporate) that depend on these systems. Technical levels are critical to systemic cybersecurity, but not necessarily dependent on government intervention [21].

Cybersecurity policy implements key values: security, privacy, fairness, economic value and accountability. Security defines the protection of assets (tangible and intangible) from harm. Loss of accessibility, integrity and disclosure of assets privacy lead to a reduction in the value to the asset owners. Privacy allows stakeholders (individuals, groups, organizations) to restrict information about themselves, including the concept of proper use and protection of information. Justice is implemented by a symmetric (necessary) policy on the subjects, including due process. Economic value is profit caused or stopped by a policy choice. Accountability is the degree to which entities (public and private) can be held responsible for the consequences of their actions or inactivity [11].

The Global Cybersecurity Index (GCI) is included in the ITU 130 International Telecommunication Union (ITU) Plenipotentiary Resolution (Dubai, 2018) on enhancing ITU's role in building trust and security in the use of information and communication technologies. Member-states are invited to support ITU initiatives in the field of cybersecurity, including the Global Cybersecurity Index (GCI), to promote national strategies and exchange of information on branch and sectoral actions. It should be noted that, based on research and proposals, Estonia and Poland have already adopted cybercrime laws, Zimbabwe, Zambia, Egypt, South Africa have developed cybercrime legislation. At the organizational level, some countries (Australia, Botswana, Canada, Czech Republic, Denmark, Japan, Jordan, the Netherlands, Spain, Samoa, Singapore and Luxembourg) have updated national cybersecurity strategies. Cybersecurity approaches based on risk assessment allow us to adjust the changing threats faced by each country, but the study shows that only 92 (about 53%) of countries conduct cybersecurity risk assessments [22].

The National Cybersecurity Index (NCSI) is a global index that measures countries' readiness to prevent cyber threats and cybercrime. In addition to the NCSI index, the index table also displays the level of digital technology development (DDL). The difference shows the relationship between NCSI score and DDL. A positive result means that the development of cybersecurity in the country is in line with or ahead of its digital development. A negative result shows that the digital society in the country is more developed than the sphere of national cybersecurity. Fig. Figure 2 shows the relevance of digital development to counteract cyber threats (as determined by NCSI), according to 2019. Ukraine ranked 26th among 131 countries in the National Cybersecurity Index (63.64) [23].

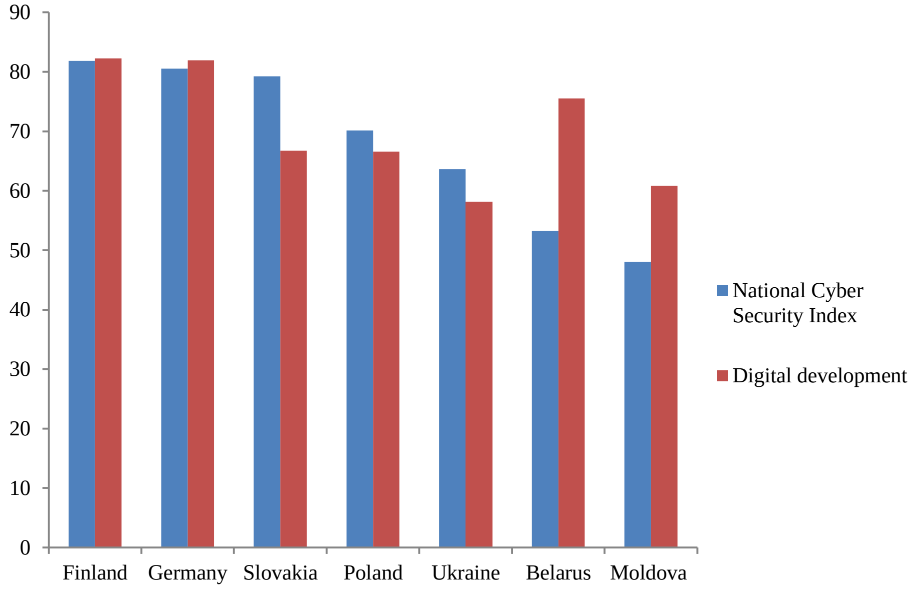

Fig. 2. Digital development relevance of some countries to respond cyber threats (Source: [23])

2 Developing a public-private partnership for cybersecurity

Issues related to policymaking in the sphere of cybersecurity and the factors behind its implementation testify to the inability of government functions to ensure the security of information networks, critical infrastructures, and storage of information content. The need to involve a private partner in solving existing and emerging threats to critical infrastructures, reducing vulnerabilities, protection of state electronic services, limitation of financial and technological resources, and supporting the security life cycle envisages implementing public-private partnership mechanisms into the projects related to cybersecurity and cyber threats counteraction. Considering international experience, PPP mechanisms give hope for the success of public and private sector cooperation strategies in cybersecurity.

S. Linder views PPP output as a synergistic effect of sharing innovative resource use and an application of management knowledge that optimally allows to achieve the goals of all participants, if such goals cannot be achieved without involving these participants. [24].

M. Carr emphasizes the need for a market-based approach to PPP cooperation in cybersecurity, which is part of national security [25]. Thus, in the process of PPP, security responsibilities are delegated to the private sector in accordance with market principles. [26, p. 299].

T. Moore [27] proposes to divide cybersecurity areas where PPP can be applied into four main areas:

- online identity theft;
- industrial cyber espionage;
- protection of critical infrastructure;
- botnets.

These vulnerabilities may be areas of joint activity of the state and private entities within PPP models, but this cooperation is now in a much wider range. The use of PPPs may involve cybersecurity projects related to the use of ICTs in various areas of government, local self-government, given the Copenhagen School's definition of security zones: military, political, social, economic and environmental [28] and critical infrastructure protection, including: agriculture and food systems, energy systems, medical institutions, banking and financial systems, commercial facilities and shipping services, the most of which are privately owned [29].

Public security agencies in many countries around the world have increasingly involved the private sector in managing various national security issues in order to implement a policy of minimizing risks and ensuring the society resilience to threats, natural disasters and man-made disasters [30]. Cybersecurity involves public-private partnership [31], as highlighted by policy initiatives and public statements on the value of public-private partnerships for cybersecurity [32].

S. Linder [33] considers the use of public-private partnerships in cybersecurity as a reform of governance and as a separation of power. In the first case, the researcher hopes for the opportunity of the authorities to reproduce the best opportunities of the private partner in terms of business skills, flexibility and other innovative approaches. There is an opinion on the need to protect the private sector's interests on its own merits and opportunities, given the lack of full capacity for this in the public sector [34]. On the other hand, the public interest in cybersecurity may not be in line with the private sector, since it affects profit-related issues [35, p. 53]. Certain actions to protect your own infrastructure can ultimately produce positive results in the form of revenue.

The separation of power between the partners entails the principles of trust, responsibility and risk sharing, which underpin public-private partnership contracts. Close partnership requires the sharing of private data that contain private-sector commercial information, and restricted or state-secret information available to a public partner.

EU strategic documents on cybersecurity highlight the role of PPP, which combines private sector cooperation in the fight against cybercrime [36]. The European Union Agency for Cybersecurity (ENISA) has published Good Practice Guide with specific guidance for public and private parties on the creation and operation of PPPs in cybersecurity [37]. In 2018 study [38] ENISA offered its own vision for PPP cybersecurity models, identifying four major model solutions: Institutional PPP based on a common approach that provides services and protects critical infrastructure against cyber threats; Goal-oriented PPP that develops cybersecurity in EU Member States; Service outsourcing PPPs address the issues of a particular industry in case stakeholders cannot resolve them independently; Hybrid PPPs are a combination of institutional and outsourced PPPs when needed at national level.

Following the Cybersecurity Act (Regulation 2019/881) entry into force, ENISA has been commissioned to prepare the *European Cybersecurity Certification Scheme* guidance that serve as a basis for certification of products, processes and services that support Digital Single Market. The European Cybersecurity Law establishes rules and European schemes for cybersecurity certification of ICT products, processes and services [39].

In modern practice, the challenges of public-private interaction in the field of cybersecurity are proposed: reliable Internet access interfaces (ICTs); joint regulation of technical security and data processing; exchange of information on threats and vulnerabilities; mutual assistance in addressing known threats or illegal content in cyberspace [40, p. 227]. In partnership, private enterprises are called upon to voluntarily share their knowledge of national security and to take responsibility for ensuring effective cyber-threat management [25].

The US Department of Homeland Security (DHS) has created an automated cyber-threat program to facilitate the rapid and timely sharing of threat information between the public and private sectors. DHS has introduced Automated Indicator Sharing (AIS) for the automated exchange of metrics between the public and private sectors, using a common query from large companies when sharing information is one-sided; threats at network speeds are resolved almost from the moment they occur [11].

Hybrid interaction between the state and the private sector on the basis of PPP cybersecurity projects makes it possible to replace the functions of control, coordination and motivation of fulfilling security tasks by partially fulfilling them by the interested private partner. In the process of managing cyber defense procedures, it is necessary to investigate threats and their evolution, to look for vulnerabilities, to determine transfer and incorporation of the goals and priorities; to outsource; to prevent and maintain, to response to attacks; to check the effectiveness of actions. Considering the complexity of this issue, the implementation of cybersecurity through the use of PPPs envisages the involvement of business entities using ICT-dependent critical infrastructure elements as a private partner; manufacturers of server equipment, developers of software products, payment service providers [1]. These issues should include the strategic planning of government activities, the formation of the necessary institutions, the development of procedures and processes, compliance with the interests of the parties, improvement of the management of public-private partnerships development in the field of cybersecurity.

3 Conclusions

The processes that dictate cybersecurity measures for information infrastructure are quite complex. Existing methods of state regulation of the security sector are rapidly losing their relevance, given their low efficiency. A modern approach to cybersecurity solutions based on public-private partnership models is a new form of governance. But the implementation of certain functions of the state with the help of the private sector can be seen through the lens of finding the best actions between maintaining security and making a profit and information sharing and confidentiality of information. The tasks that need to be addressed with regard to the further development of PPPs in the field of cybersecurity are: legislative implementation of cybercrime rules, protection of critical infrastructures, data exchange protocols in the process of critical infrastructures protection; implementation of standardization adopted in the EU; regulation of technical security and data processing; assistance in resolving situations involving threats or illegal content on the Internet. Developing opportunities for cooperation between the state and private actors in the field of cybersecurity based on PPP models depends on future priority projects, increase of mutual trust, a strategy in the field of critical infrastructure security, standardization, cooperation with partners.

References

1. Kruhlov, V. V.: Public-private partnership in the field of cybersecurity. “Scientific Notes of Taurida V. I. Vernadsky University”, series "Public Administration 29(68), 57–61 (2018).
2. Schwab, K.: The fourth industrial revolution. Crown Publishing Group, New York (2017).
3. 2018: Data Privacy and New Regulations Take Center Stage, https://breachlevelindex.com/, last accessed 2019/10/23.
4. Here are the biggest cybercrime trends of 2019, https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/, last accessed 2019/10/23.
5. Asen, A., Bohmayr, W., Deutscher, S., Gonzalez, M. and Mkrtchian D.: Are You Spending Enough on Cybersecurity?, https://www.bcg.com/en-gb/publications/2019/are-you-spending-enough-cybersecurity.aspx, last accessed 2019/10/23.

6. There's Nowhere to Hide from the Economics of Cybercrime, https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html, last accessed 2019/10/23.
7. Global Cybersecurity Index 2018, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf, last accessed 2019/10/23.
8. AI is the latest weapon cybercriminals are exploiting, https://www.weforum.org/agenda/2019/09/4-ways-ai-is-changing-cybersecurity-both-in-attack-and-defense/, last accessed 2019/10/23.
9. Wells, D., Brewster, B., Akhgar, B.: Challenges priorities and policies: mapping the research requirements of cybercrime and cyberterrorism stakeholders. Combatting Cybercrime and Cyberterrorism. Springer, Cham 39–51 (2016).
10. Schwab, K.: The Fourth Industrial Revolution: what it means, how to respond, World Economic Forum, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/, last accessed 2019/10/23.
11. Cyber Resilience. Playbook for PublicPrivate Collaboration. WEF (2018).
12. Internet Security Threat Report, volume 22. April 2017, https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf, last accessed 2019/10/23.
13. The Global Risks Report 2018. 13th Edition. Geneva (2018).
14. Klimburg, A.: National cyber security framework manual. NATO Cooperative Cyber Defense Center of Excellence Publication. Tallinn (2012).
15. e Silva, K.: Europe's fragmented approach towards cyber security. Internet Policy Review 2(4) (2013).
16. Christensen K. K., Petersen K. L.: Public-private partnerships on cyber security: a practice of loyalty. International Affairs 93(6), 1435–1452. (2017).
17. Coats, D. R.: Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence. Office of the Director of National Intelligence. United States (2017).
18. Kim, J.: Cyber-security in government: reducing the risk. Computer Fraud & Security 7, 8–11 (2017).
19. Mueller, M., Schmidt, A., Kuerbis, B.: Internet security and networked governance in international relations. International Studies Review 15(1), 86–104. (2013).
20. Von Solms, R., Van Niekerk, J.: From information security to cyber security. Computers & Security 38, 97–102 (2013).
21. DeNardis, L.: Hidden levers of Internet control: An infrastructure-based theory of Internet governance. Information, Communication & Society 15(5), 720–738 (2012).
22. Global Cybersecurity Index (GCI) 2018, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf, last accessed 2019/10/23.
23. National Cyber Security Index, https://ncsi.ega.ee/compare/, last accessed 2019/10/23.
24. Linder, S., Rosenau, V. P.: Mapping the terrain of the Public-Private Policy Partnership. Public-Private Policy Partnerships. P. V. Rosenau (Ed.). The MIT Press, Cambridge, MA (2000).
25. Carr, M.: Public-private partnerships in national cyber-security strategies. International Affairs 92(1), 43–62 (2016).
26. Bures, O. Contributions of private business to the provision of security in the EU: beyond public-private partnerships. Crime, Law and Social Change 67(3), 289–312 (2017).

27. Moore, T.: Introducing the Economics of Cybersecurity: Principles and Policy Options. Deterring Cyberattacks: Informing Strategies and Developing Options for U. S. Policy, https://www.nap.edu/read/12997/chapter/3, last accessed 2019/10/23.
28. Buzan, B., Waever, O., De Wilde, J.: Security: a new framework for analysis. Lynne Rienner Publishers (1998).
29. O'Rourke, T. D.: Critical infrastructure, interdependencies, and resilience. The Bridge. Washington: National Academy of Engineering 37 (1), 22–29 (2007).
30. Carrapiço, H., Barrinha, A.: The EU's emerging security actorness in cyberspace: Quo vadis? The EU, Strategy and Security Policy. Routledge, 104–118 (2016).
31. Tropina, T.: Public-private collaboration: Cybercrime, cybersecurity and national security. Self-and co-regulation in Cybercrime, cybersecurity and national security. Springer, Cham, 1–41 (2015).
32. Min, K. S., Chai, S. W., Han, M.: An International Comparative Study on Cyber Security Strategy. International Journal of Security and Its Applications № 9(2), 13–20. (2015).
33. Linder, S. H.: Coming to terms with the public-private partnership: A grammar of multiple meanings. American behavioral scientist 43(1), 35-51 (1999).
34. Holder, E. Jr.: Deputy Attorney General, US Department of Justice, prepared statement for 'Internet Security' (2000).
35. Stiglitz, J. E., Wallsten, S. J.: Public-private technology partnerships: Promises and pitfalls. American Behavioral Scientist 43(1), 52–73 (1999).
36. Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels (2013).
37. Good Practice Guide on Cooperative Models for Effective Public Private Partnerships. Uropean Network and Information Security Agency (ENISA) (2011).
38. Public Private Partnerships (PPP). Cooperative models. ENISA. 2018, https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models, last accessed 2019/10/23.
39. About ENISA, https://www.enisa.europa.eu/about-enisa, last accessed 2019/10/23.
40. Bossong, R., Wagner, B.: A Typology of Cybersecurity and Public-Private Partnerships in the Context of the European Union. Security Privatization. Springer, Cham (2018).