Discussion Paper
Nº 04 • JANUARY 2021

Achieving robust European cybersecurity through public-private partnerships:
Approaches and developments

Francesco Cappelletti
Research Fellow, European Liberal Forum

Prof. Luigi Martino
PhD, Professor of Cybersecurity and International Relations, University of Florence

The opportunities offered by cyberspace and information and communication technologies have changed how businesses operate, governments function, and people live. Nevertheless, it has become clear that Member States need to equip themselves with the necessary technical and regulatory tools to counter cyber threats. In this context, the cooperation between the public and private sectors could prove crucial in order to stimulate such developments and foster the European cybersecurity market and strategy.

Cybersecurity; public-private partnership; European Union; liberalism;

Content

Authors' Bios

Francesco Cappelletti is Research Fellow at the European Liberal Forum. After obtaining his master's degree at the University of Florence and the Moscow State Institute of International Relations, he worked as a freelance consultant in the field of International Relations and Security, managing projects in Europe, Russia, and the Middle East. He collaborates with different research centres (CCSIRS – Florence, RIAC – Moscow) and is a member of Fondazione Luigi Einaudi (Rome).

Luigi Martino (PhD) teaches Cyber Security and ICT Policies at the Faculty of Political Science "Cesare Alfieri" in Florence and is head of the Center for Cyber Security and International Relations Studies (CCSIRS). His PhD thesis at the Scuola Superiore Sant'Anna in Pisa focused on the implementation of cybersecurity models for the protection of national infrastructures through public-private partnerships. From 2016 to 2018, he was project manager of the OSCE research project "Enhancing the Implementation of Conflict Stemming from the Use of ICTs". He is a member of the Research Advisory Group of the Global Commission on the Stability of Cyberspace and is Director of the CCSIRS-Unifi node of the CINI National Cybersecurity Laboratory.

Publisher
European Liberal Forum

European Liberal Forum asbl
Rue d'Idalie 11-13, boite 6
1050 Ixelles, Brussels (BE)

Contacts:
+32 (0)2 669 13 18

info@liberalforum.eu

www.liberalforum.eu

Cover Image:
© [RVNW]/Adobe Stock

Graphic design: epiquestudio.com

ISSN: 2684-6667

Published by the European Liberal Forum asbl. Co-funded by the European Parliament. Neither the European Parliament nor the European Liberal Forum asbl are responsible for the content of this publication, or for any use that may be made of it. The views expressed herein are those of the author(s) alone. These views do not necessarily reflect those of the European Parliament and/or the European Liberal Forum asbl.

Executive Summary

Today the opportunities offered by cyberspace and information and communication technologies (ICT) provide significant benefits that have changed how businesses operate, governments function, and people live. The relatively recent birth of this new dimension has also affected inter-state relations and, more broadly, the dynamics of the international arena. Notwithstanding the relevant positive effects enabled by the information revolution, according to empirical evidence, there is a "dark side" of cyberspace. In recent years, European cybersecurity regulations have seen an unprecedented development, providing the legal basis for a future in which the cyber domain and environment is independent in terms of its innovative capacity, security, and resilience. Nevertheless, it has become clear that Member States need to equip themselves with the necessary technical and regulatory tools to counter cyber threats. This should result in strategic area investments and, when in place at the European Union level, these could be the key for optimising development in the field. Consequently, the mixed convergence of private ownership/management of cybersecurity skills, as well as public and private obligations and responsibilities, have convinced policymakers to consider the "partnership" between public and private stakeholders (i.e., public-private partnerships, PPPs) as the correct remedy for mitigating cyber risks and strengthening security. This cooperation between the public and private sectors could prove crucial in order to stimulate such developments and foster the European cybersecurity market.

The first part of this Discussion Paper, by Prof. Luigi Martino, takes into account the regulatory aspect of collaborations with private actors in the European context. It shows that improving the implementation of regulations and frameworks is a fundamental step in achieving a strong cybersecurity structure. The second part, by Francesco Cappelletti, analyses the characteristics of PPPs in the cybersecurity field within the broader context of cooperation with the private sector and examines how this could stimulate the development of the European cybersecurity market while following a liberal approach.

Both in terms of the market and fair accessibility (especially for small and medium enterprises, SMEs), a liberal approach is the optimal solution to the long-standing issues of accountability, reliability, and relationships between parties. At the same time, as the authors argue, PPPs in the field of cybersecurity need to be guided by a regulatory framework that favours their development while also ensuring the protection of citizens' rights.

Chapter 1

The diffusion of PPPs on cybersecurity and protecting critical infrastructures from cyber-attacks: The European Union approach

Prof. Luigi Martino
PhD, Professor of Cybersecurity and International Relations, University of Florence

The question of defining specific policies for critical infrastructure protection (CIP) has been debated by European institutions since the beginning of the twenty-first century. Immediately after the 9/11 terrorist attacks in the United States, and the terrorist attacks on EU territory (Madrid 2004 and London 2005)[1], the European Commission started a debate on how to protect those infrastructures which, in case of attacks or incidents, would have an impact on the safety of citizens and the security of Member States.[2]

Hence, in EU policy documents the term "resilience" arose as a key element of critical infrastructures (CIs) in relation to the strategic priority to guarantee service (or business) continuity in case of destructive and unpredictable events.[3] The EU Cybersecurity Strategy (2020) also recalls this broad understanding of the term, encompassing all relevant sectors, public and private, that perform an important function for the economy and society.[4]

[1] United Nations Office of Counter-Terrorism and United Nations Counter-Terrorism Committee Executive Directorate, The protection of critical infrastructures against terrorist attacks: Compendium of good practices, 2018, pp. 91, 109.

[2] See R. Setola, E. Luiijf, and M. Theocharidou, "Critical Infrastructures, Protection and Resilience", in Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, eds. R. Setola, V. Rosato, E. Kyriakides, and E. Rome, Springer, Berlin, 2016, pp. 1-18; European Commission, Network and Information Security: Proposal for A European Policy Approach, COM(2001) 298, 6 June 2001, p. 9; H. Carrapico and A. Barriha, "The EU as a Coherent (Cyber)Security Actor?", JMS 55, no. 6, 2017, pp. 1254-1272.

[3] B. Hämmerli and A. Renda, "Protecting Critical Infrastructure in the EU", CEPS Task Force Report, Brussels, 2010, p. 15 et seq.; C. Pursiainen and P. Gattinesi, "Towards Testing Critical Infrastructure Resilience", JRC Scientific and Policy Reports, 2014, pp. 14-17.

[4] European Commission, High Representative of the Union, Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020)18, 16 December 2020, p. 5.

The Commission even established the European Programme for Critical Infrastructure Protection (EPCIP), acknowledging the relevance of proactive cooperation between the owners and operators of critical infrastructures (both public or private) and the national authorities of Member States.[5] In particular, the main goals of the EPCIP are based on three key strategic areas:

a) creating a procedure for the identification and designation of European Critical Infrastructures (ECI) and a common approach to the assessment of such infrastructures' protection when improvements are needed;
b) designing measures to facilitate the implementation of the EPCIP, including an EPCIP Action Plan and the Critical Infrastructure Warning Information Network (CIWIN) funding projects on this specific issue;
c) establishing international collaboration between the European Economic Area (EEA), the European Free Trade Area (EFTA), and the United States and Canada.

Indeed, regarding the concept of critical infrastructure protection, the *Green Paper On A European Programme For Critical Infrastructure Protection* outlined the need to guarantee "business continuity" of services provided by critical infrastructures as well as to protect citizens of the Union from terrorist attacks.[6]

The responsibility issue, which is being used as a lever by European policymakers to establish appropriate models of collaboration between public and private sectors, was established in the Commission communication that states ensuring CIP "[...] *is a shared responsibility: no single stakeholder has the means to ensure the security and resilience of all* [...] *infrastructures and to carry all the related responsibilities*".[7]

[5] European Commission, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786, 12 December 2006.
[6] European Commission, Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576, 17 November 2005, p. 2.
See also G. Christou, Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy, Palgrave Macmillan, London, 2016, p. 122.
[7] European Commission, Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, SEC(2009) 399, 30 March 2009, p. 5.

The responsibility issue was also raise by the Council resolution of the same year on a collaborative European approach to network and information security, which emphasizes that "[...] *the ICT sector is vital to most sectors of society, making Network and Information Security a joint responsibility of all stakeholders, including operators, service providers, hardware and software providers, end-users, public bodies and national government.*"[8]

To the issue of collaboration with the private sector, the same resolution adds: "*The importance of an active and knowledgeable European Network and Information Security community that contributes to the increased collaboration between Member States and the private sector*".[9]

> "The Council [...] indicates PPPs as the necessary instrument to mitigate, prevent, and provide an appropriate European response to the risks deriving from attacks on networks and information systems

In other words, the Council not only identifies the crucial role of the private sector to ensure the robustness and the resilience of critical infrastructures in case of incidents or attacks (i.e., business continuity) but also indicates PPPs as the necessary instrument to mitigate, prevent, and provide an appropriate European response to the risks deriving from attacks on networks and information systems, recognizing: "[...] *the importance of multi-stakeholder models such as Public Private Partnerships (PPPs), built on a long term, bottom-up model to mitigate identified risks where such an approach delivers added value in helping to ensure a high level of network resilience*".[10]

In this framework, the Commission establishes the conditions for creating an action plan in order to implement PPPs for the protection of CIs from cyber-attacks (the CIIP Action Plan). Several scholars have considered the ISAC (Information Sharing and Analysis Centre) model as a reference for the creation of a common platform between the public and private sectors for exchanging information. The ISAC was originally born in the United States in 1997 after the first attempted terrorist attack on the World Trade Center in 1993 and the 1995 events in Oklahoma City.[11] It is important to note that the European Union approach—prior to Directive 2008/114 (the ECI Directive) and even up to Directive 2016/1148 (the NIS Directive)—until quite recently did not provide effective collaboration mechanisms between public and private actors, nor among Member States in the context of critical infrastructures protection.[12]

[8] Council of the European Union, Council Resolution on a collaborative European approach to Network and Information Security (2009/C 321/01), 18 December 2009, section III, 2.

[9] Ibid., section IV, 1.

[10] Council of the European Union, section IV, 7.

[11] See N. Choucri, S. Madnick, and P. Koepke, "Institutions for Cyber security: International Responses and Data Sharing Initiative" (working paper), Cybersecurity Interdisciplinary Systems Laboratory, Massachusetts Institute of Technology, August 2016; J. Korte, "Mitigating cyber risks through information sharing", Journal of Payments Strategy & Systems 11, n. 3 (Fall 2017), pp. 203-214; European Union Agency for Cybersecurity (ENISA), "Information Sharing and Analysis Centres (ISACs). Cooperative models" (2018); A. Mermoud et al., "To share or not to share: a behavioral perspective on human participation in security information sharing", Journal of Cybersecurity 5, No. 1 (June 2019), pp. 1-13.
For more info about ISAC, the EU, and PPPs, see E. Ouzounis, "PPP and ISAC in the EU" presentation, Attiki, 14 December 2018.

[12] A. Rotondo, "Cybersecurity e protezione delle infrastrutture critiche: l'efficacia del modello europeo", in Lo spazio cyber e cosmico: risorse dual use per il sistema Italia in Europa, eds. S. Marchisio and U. Montuoro, Giappichelli Editore, Turin, 2019, p. 127.

The main reason the Commission has identified for considering PPPs as a useful tool in this context is the result of a simple but practical syllogism consisting of a premise and two consequences: (a) the private sector "owns or controls" a large number of critical infrastructures; (b) the implementation of security policies depends on the involvement of the private sector in the "*definition of strategic public policy objectives as well as operational priorities and measures*"; (c) PPPs "*would bridge the gap between national policy-making and operational reality on the ground*".[13]

It is important to note that, in the EU regulatory framework (at an operational level), the concept of PPP applied to the protection of critical infrastructures from cyber-attacks is based on the actions carried out by ENISA (European Union Agency for Cybersecurity) and EUROPOL (European Police Office). In particular, these two EU bodies contribute to collaborations with national public authorities, European institutions, and the public or private sectors which are included in the CIP framework. These collaborations are organised mainly to facilitate the exchange of information and assistance and for the purpose of implementing the common standards of information sharing in the national legal systems.[14]

ENISA's collaborations with the private sector aim to increase, from a technical point of view, the reliability and resilience of cyberspace and critical infrastructures. EUROPOL, on the other hand, sustains collaborations related to information sharing, according to the specific purposes of a law enforcement agency. EUROPOL has implemented specific PPPs aimed at fighting cyber-crime through the creation of support groups for the EC3 (European Cybercrime Centre) with a specific focus on operational rather than security aspects and a specific law enforcement-oriented approach. As Bossonf and Wagner claim, the EC3 signed several memoranda of understanding (MoU) with private operators in two specific sectors: finance and ICT. On the side of active assistance, the formalization of PPPs follows the general goal of risk sharing. In addition to the exchange of information, cooperation with IT companies on the operational level is structured to include specific tasks such as criminal investigation, trojan elimination, and botnet detection.[15]

In the action against the Shylock trojan in July 2014, for example, the EC3 directed their operations thanks to the support of the NCA (National Crime Agency) of the United Kingdom, the FBI (Federal Bureau of Investigation) of the United States, and police agencies from the Netherlands, Italy, Turkey, Germany, Poland, and France, as well as the Symantec Corporation. It is also noteworthy that Microsoft, along with other companies, participated in the action campaign coordinated by the EC3 against the Ramnit botnet. Thanks to the Microsoft IoT (internet of things) suite, it was possible to group and analyse data in near-real time and monitor this threat.

[13] Ibid.
[14] R. Bossong and B. Wagner, "A typology of cybersecurity and public-private partnerships in the context of the EU", Crime Law and Social Change 67, 2017, p. 267.
[15] See Ibid., p. 280.; C. Osborne, "Police, security firms team up and take down Skylock malware", ZDnet, 11 July 2014; J. Hardoy, "Breaking Up a Botnet – How Ramnit was Foiled", Microsoft EU Policy Blog, 22 October 2015.

In this political-regulatory context, the European Public Private Partnership for Resilience (EP3R) emerges as a strategic programme at the pan-European level in order to develop and use PPPs in the context of critical infrastructures, especially in the telecommunications sector.[16]

> “The EU approach has identified [...] the PPP model as an appropriate tool to combine joint efforts and capabilities [...] in a multi-stakeholder governance framework

The EU approach has identified, especially through the EP3R programme, the PPP model as an appropriate tool to combine joint efforts and capabilities in an open and inclusive cooperation between public and private actors who are all included in a multi-stakeholder governance framework.[17]

However, the lack of operational activities of the European “PPP model” has proven to be the weakness of the EP3R. Indeed, the absence of a key political role in the regulatory instruments of CI operators (particularly private actors) and the exclusivity of political authorities in defining means and goals have hampered the activities of this partnership—with negative effects both on results and on the policies of regulating and including private actors in decision-making processes.[18]

It is no coincidence that the European cyber security strategy of 2013 referred to the EP3R as a tool “*to be implemented.*”[19] At that time, European policy makers re-affirmed the concept of shared responsibility between public and private actors in identifying the “*vulnerabilities of European critical infrastructure and encouraging the development of resilient systems.*” [20]

> “The lack of operational activities of the European “PPP model” has proven to be the weakness of the EP3R

Moreover, the draft proposal of the NIS Directive has stressed, among other goals, the implementation of specific policies focused on private sector cooperation—including specific recommendations to the national authorities dictating the necessary measures to “improve preparedness and engagement of the private sector”.[21] This cooperation will also build upon the progress made in the context of the “European Forum for Member States (EFMS), which has held productive discussions and exchanges on NIS public policy and can be integrated in the cooperation mechanism once in place”. It specifies that:

[16] S. Purser, “The European cooperative approach to securing critical information infrastructure”, Journal of Business Continuity & Emergence Planning 5, No. 3, Fall 2011, pp. 237-245; K. Irion, “The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R)”, in The Secure Information Society, eds. J. Krüger, B. Nickolay, S. Gaycken, Springer, London, 2013, pp. 83-116; M. Dunn Cavelty, “A Resilient Europe for an Open, Safe and Secure Cyberspace”. *UI Occassional Papers*, No. 23, December 2013.

[17] R. Bossong, B. Wagner, p. 276.

[18] Ibid., p. 277.

[19] European Commission, High Representative of the Union, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013)1, 7 February 2013, p. 7.

[20] Ibid., pp. 2, 4.

[21] Ibid., pp. 5-6. The strategy was also accompanied by a proposal for legislation to establish a high common level of network and information security (i.e., the NIS Directive). European Commission, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(213)48, 7 February 2013.

"Since the large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cybersecurity is crucial. The private sector should develop, at technical level, its own cyber resilience capacities and share best practices across sectors. The tools developed by industry to respond to incidents, identify causes and conduct forensic investigations should also benefit the public sector." [22]

In this respect, the Commission identifies specific forms of collaborations between public and private sectors and suggests the creation of "PPPs as platform" to involve all (public and private) stakeholders in sharing best practices from the field of cyber security and developing incentives to facilitate the implementation of measures needed to secure and protect critical infrastructures. In order to achieve the abovementioned purposes, the ENISA has created, inside the NIS platform framework, three working groups, with a specific focus on co-regulatory tools and related public policies with reference to risk management, information sharing and coordination in case of incidents between public and private actors.[23]

Therefore, ENISA developed an ideal PPP model for the protection of critical infrastructures from cyber-attacks based on the European policy framework. Indeed, ENISA's premise is that:

"The large number of PPP experiences worldwide has confirmed the value of such approach also for its flexibility and appropriateness for today emerging challenges including cyber-attacks mitigation, critical infrastructure protection and security and resilience of information and communications".[24]

At the same time, European policy makers, aware of the need to promote a bottom-up process of policy building,[25] have encouraged all actors involved in the critical infrastructure or essential service ecosystems to develop informal and formal collaboration mechanisms with governmental authorities in order to ensure critical infrastructures' adequate protection, especially from cyber risks.[26]

European policy makers [are] aware of the need to promote a bot- tom-up process of policy building

[22] Ibid.
[23] European Commission, Cybersecurity Strategy of the European Union, p. 14.
See also R. Bossong, B. Wagner, p. 277.
[24] See European Union Agency for Cybersecurity (ENISA), EP3R 2009-2013 Future of NIS Public Private Cooperation, 2015.
[25] R.E. Matland, "Synthesizing the Implementation Literature: The Ambiguity-Conflict Model of Policy Implementation", Journal of Public Administration Research and Theory, No. 5, April 1995, pp. 145-174.
[26] Cybersecurity Strategy of the European Union, p. 13.

The Commission's approach is as simple as it is practical. On the one hand, the rules for operators can considerably improve the protection of citizens, businesses, and European institutions against risks to critical infrastructures or essential services.[27] The regulatory approach of the NIS Directive is not so much about the reliability of the processes provided by the Directive itself, but rather about the formalization of the collaboration between the public sector and the private sector compared to the obligations and security measures provided.[28] On the other hand, *"the introduction of requirements to implement NIS [Network Information Security] risk management for public administrations and key private players would create a strong incentive to manage security risks effectively"* and, in the long term, would favour the development of an ecosystem based on the model of PPP governance. *"In particular, the obligations placed on the Member States would ensure adequate preparedness at national level and would contribute to a climate of mutual trust, which is a precondition for effective cooperation at EU level".*[29]

In this view, on 16 December 2020, the Commission proposed: to replace the ECI Directive, expanding the sectors involved and in conjunction with the reform of the NIS Directive; to increase the level of cyber resilience of critical sectors, public and private, that perform an important function for the economy and society; and to introduce a risk management approach, including cyber risk in the supply chain.[30] Moreover, the EU's Cybersecurity Strategy for the Digital Decade, as a joint initiative of the European Commission and the High Representative for Foreign Affairs and Security Policy, was released on the same day. It focuses on public-private partnerships as a tool to unlocking investments, supporting a cyber-secure digital transformation, and increasing the level of cyber resilience of critical sectors.[31]

> "[The 2020] EU's Cybersecurity Strategy for the Digital Decade […] focuses on public-private partnerships as a tool to un- locking investments, supporting a cyber-secure digital transformation, and increasing the level of cyber resilience of critical sectors.

[27] H. Carrapico, A. Barriha, p. 1265.
For more info about contractual PPP, see European Commission, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016)410, 5 July 2016, pp. 12-13; P. Timmers, "The European Union's cybersecurity industrial policy", Journal of Cyber Policy 3, No. 3, November 2018, pp. 363-384.
[28] European Commission, Strengthening Europe's Cyber Resilience System..., p. 3.
[29] European Commission, Proposal… to ensure a high common level of network and information security..., pp. 7-8.
[30] European Commission, Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities, COM(2020)829, 16 December 2020; European Commission, Proposal for a Directive of the European Parliament and the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020)823, 16 December 2020, p. 7.
[31] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, p. 5.

Conclusion and recommendations

Encourage, Gather, Optimise: the PPP approach should aim at optimizing functions and respecting the actors' specific characteristics, avoiding any dispersion of efforts which may lead to possible duplications on the part of other organisations or other forms of PPPs. Another key point is related to the role of government or public authorities, which should be mainly directed at reducing barriers to entry into the PPP framework and encouraging the private sector's active participation.

Aim at a Bottom-up Approach: PPP governance should initially be based on a top-down model that later, according to the numerical growth of PPP actors involved, should move to a bottom-up model—where newly introduced initiatives should not be adopted via a centralized approach, under the prominent influence of public or governmental authorities, but should be brought in based on common will among the "community of participants".

Look for Added Value: private sector participation should be preferred when it adds a clear value in terms of technical skills that can also be translated into some significant contribution (if required by national legislation) wherein private entities participate in the management of cyber crises that can have deleterious effects on citizens' safety or national security.

Indeed, the involved actors' intentions to prevent, mitigate, and react to cyber threats provide for the coordination of both public and private sector efforts. The organisational or institutional architecture, through the designated mechanisms and actors involved, can determine the analysis of a given threat, the collaboration between states, and the ability to respond effectively.[32] In the European context, for instance, these aspects could be included in the concept of "shared responsibility" which, as stated above, is at the basis of the PPP concept itself. [33]

Willingness and interests: these two points deserve additional emphasis. The first concerns the willingness of Member States to share responsibility and capabilities (i.e., power factors) on a decisive aspect of their survival (i.e., cyber security). The second concerns attempts to absorb the tensions lying between the different interests of public and private actors. For both points, the combination of governance mechanisms offered by PPPs (i.e., the multi-stakeholder approach) seems to allow for the recognition of decentralization (i.e., distribution of practices and powers), of the cross-border and supranational nature of the problem, and of the effects of the decision-making process in terms of its complex causal dynamics (i.e., uncertainty caused by cyber incidents, or CIs, by default). Therefore, the ability to respond can ultimately be strengthened by the PPP governance approach, which favours the application of measures and policies to increase the protection of critical infrastructures and essential services and facilitates, inter alia, information-sharing mechanisms with the private sector.

The PPP approach applied to the CIP context, as recommended by ENISA, would

[32] T. Chaudhary, et al., "Patchwork of confusion: the cybersecurity coordination problem" (research paper), Journal of Cybersecurity, August 2018, pp. 1-13.
[33] See S. Piattoni, "Multi-level Governance in the EU. Does it Work?", Globalization and Politics – A Conference in Honor of Suzanne Berger, Massachusetts Institute of Technology, May 2009.

lead to the development of a virtuous circle based on an "osmotic" relationship between the various stakeholders that, inter alia, would allow each sector and each layer to increase—in a coordinated manner—its capacity for prevention, response, and recovery in the event of a crisis triggered by an incident or cyber-attack against critical infrastructure, thus increasing shared situational awareness across the EU.[34]

With that in mind, in order to strengthen PPPs at the European level and to enhance security and resilience:

- Due to the nature of cybersecurity and cyber-attacks, which could be highly interconnected and interdependent, this issue should be addressed at a supranational level.
- A PPP model should allow for the exchange of knowledge and best practices in order to build a common base among all stakeholders, including innovative SMEs, researchers, and academics.
- Cooperation with the private sector, being a key point from an investment perspective, could be influenced by regulatory actions.
- The PPP approach should aim at optimizing functions and respecting the actors' specific characteristics, avoiding any dispersion of efforts which may lead to possible duplications on the part of other organisations or other forms of PPPs.
- The private sector has the competences related to networks and systems that fall within strategic objectives at the European level (e.g., the NIS Directive).
- PPPs should also be based on a clear governance framework with shared objectives that follow the principle of "shared responsibility".
- Public sector actors should reduce any economic barriers to PPP participation, as this could be a significant incentive for stakeholders to proactively participate.
- Stakeholders and participants should invest in a comprehensive and pragmatic approach towards building partnerships at the European level, where all members (public and private) get real value.
- To reach an adequate level of cybersecurity, the States should also involve those actors who, although not falling within the seven sectors identified by the NIS Directive, play a central role for the success of PPPs, for example.

[34] European Court of Auditors, Challenges to effective EU cybersecurity policy, March 2019, p. 49; European Commission, The EU's Cybersecurity Strategy for the Digital Decade, p. 3.

Comment on Chapter 1

Luigi Martino describes in detail the framework of regulations and implementations regarding PPP projects in Europe with regard to cybersecurity and its infrastructure. His chapter takes into account the regulatory aspect as the matrix of a broad context in which policies must be implemented in close collaboration with private actors. It is clear from the text that the optimisation of relationships, as well as functions, must take into account not only the rules but above all their implementation by Member States (and political actors). The idea of "optimising" the implementation of regulations and frameworks is also fundamental and, as Martino points out, one should aim to avoid creating structures that overlap one's own roles.

Finally, the described "community of participants" who should take part in a bottom-up approach, is fundamental to fostering the development of a sector market. However, the question of political will seems to remain a determining factor, as does the willingness of the Member States to share within the Union not only strategy and regulations but also their implementation. Gathering political support for a reasonable and thoughtful discussion on cybersecurity seems to be the only solution to the challenge (which, as the text shows, affects every citizen). Moreover, a liberal approach both to the market, leaving no one behind (especially SMEs), and to regulations, which must exist as a basis to support the development of a digital market. Provided there are no barriers to entry created, this could be an optimal solution.

> Gathering political support for a reasonable and thoughtful discussion on cybersecurity seems to be the only solution to the challenge

Francesco Cappelletti

Chapter 2

Free market and cybersecurity in Europe: The need for strategic public-private partnerships

Francesco Cappelletti
Research Fellow, European Liberal Forum

Introduction

The need to assist digitisation processes by providing a common cybersecurity standard within European infrastructure is the fundamental principle behind actions taken by European institutions in recent years to stimulate technological processes. While cybersecurity is a shared responsibility, integrated security by design and by default is a prerequisite for ensuring user confidence.[1]

The European project of a Digital Single Market has also fostered the development of a European framework for cybersecurity, guaranteed by certifications for products developed in the field of information and communication technologies (ICT). The creation of such a framework is a fundamental step which could actually affect the way standards are set (bottom-to-bottom or top-to-bottom).[2] From a market perspective, creating an efficient framework could potentially allow products from one country to be placed on the internal European market according to generally recognised standards and in a way that eliminates the risk of barriers and fragmentation within the single market itself.

Cybersecurity is a vital sector representing one of the EU's critical infrastructures.[3] The usability of services in the cybersecurity market depends on different technologies; therefore, the acceleration of technological processes requires a cooperative approach towards the private sector. In this regard, cooperation between industries, research centres, and universities, on the one side, and governments, on the other, is necessary for the development of the process itself. Small and medium enterprises (SMEs) and start-ups with high technological value are the key to success for a digitalisation strategy that aims at a multi-directional approach.

[1] Council of the European Union, "Shaping Europe's Digital Future" - Council Conclusions, Brussels, 9 June 2020.
[2] European Parliament, Regulation of The European Parliament and of The Council (EU 2019/881) "on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification [...] - Cybersecurity Act", 17 April 2019, title 1, art. 1.
[3] European Cyber Security Organization, "Cybersecurity in Light of Covid-19" Report, 2020, p. 13.

EU cybersecurity PPPs: Sharing security between public and private sectors

Public-private partnerships are a major model for project implementation in use, especially for the realisation of public infrastructures (such as roads, ports, airports, hospitals, energy plants, etc.). On the other hand, the private entity or entities participating in the realisation of a given project will gain income according to the type of contract. Fundamentally, these types of agreements allow the state to offload certain expenses during the execution of a project, ensuring the final product's quality through the evaluation of several projects in a public tender or based on specific agreements. Also, since such partnerships concern public service award contracts, this sort of cooperation must also be subject to specific regulations of the European Union. Broadly speaking, partnerships between public and private organisations follow some necessary procedures and definitions, widely described in the literature, that can be summarised through a few essential elements: i) solidarity, ii) mutuality, iii) commitment, and iv) sharing of responsibilities.[4]

It also is necessary, when initiating a PPP-style cooperation, to quantify the results ex-ante through indicators that guarantee the contract's optimal prospectus as well as to quantify any additional costs that might occur.[5] Another fundamental stage is the Value for Money (VFM) analysis, aimed at investigating—in the medium or long term—the efficient allocation of resources, and which can be defined as *"the optimum combination of whole-of-life costs and quality* [*of the*] *service to meet the user's requirements"*, representing a fundamental part of preventive appraisal processes.[6]

Despite what has been said so far, PPP projects in the field of cybersecurity do follow some specific rules. The same *horizontal* relationship exists, so each party involved follows the basic rule of quid pro quo. A central point, in fact, is the balance between business and security. As far as the security sector is concerned, there are numerous examples where a large part of national security is entrusted through this kind of partnership. This is also true when it comes to cybersecurity and IT infrastructure, although countries are generally less inclined to entrust network supervision to private actors.[7] Since there are certain peculiarities that cannot be assimilated to other public-private partnership contexts, there are different forms of PPP in the cybersecurity field, depending on the purpose of the partnership itself and the degree to which the parties are involved in national security issues.[8]

[4] E.H. Klijn and G.R. Teisman, "Governing Public Private Partnerships", in Public Private Partnerships: theory and practice in international perspective, ed. S.P. Osborne, Routledge, London, 2000, pp. 84-106.

[5] P. Burger, I. Hawkesworth, " How to Attain Value for Money: Comparing PPP and Traditional Infrastructure Public Procurement", OECD Journal on Budgeting, 2011, pp. 48-50.

[6] H. Martin, "Advisory Facility, Value-for-Money Analysis- Practices and Challenges", World Bank Institute, 28 May 2013, p. 9.

[7] M. Carr, "Public-private partnership in national cyber-security strategies", International Affairs, 2016, pp. 43-62. This is identified as a problem of "serious disjuncture in expectations from both 'partners'."

[8] European Union Agency for Cybersecurity (ENISA), Public Private Partnerships (PPP), Cooperative models, 2017, p. 20.

It can be said that because of the peculiarities of this type of partnership, these collaborations are not comparable to other types of PPP projects. First, the reliability of the strategic sector (i.e., cyberspace) bears considering, since a private security service provider would become the guarantor of a fundamental right—that of public and national security. On the one hand, collaboration with a private entity in this area needs to ensure the necessary crisis management capabilities.

> It can be said that because of the [cybersecurity PPPs] peculiarities, these collaborations are not comparable to other types of PPP projects.

In the other hand, outsourcing control over strategic infrastructures could potentially be perceived as a weakness in terms of strategic sectors being controlled by the central government. For this reason, "institutional" partnerships are often preferred when critical infrastructures need to be protected or when strategic sectors and private actors are involved in areas which (by law) have the public side as guarantor.[9] Such cooperation must clearly provide the preconditions for possible coordinated responses to incidents in order to make crisis management more efficient.

Second, the issue must be considered in the European context. Cybersecurity has been placed at the heart of the entire European digitalisation project, with further increased financing in the recent Recovery Plan.[10] This will be achieved by sharing part of the infrastructure and therefore (cyber) security and resiliency of the entire European cybersecurity environment at a supranational level. This quite is relevant, as the Commission not long ago affirmed the lack of an "*efficient cooperation mechanism*" for Member States when supporting cybersecurity innovation and deploying "*cutting-edge European cybersecurity solutions*".[11] In this context, cyber-PPP (cPPP) projects need to have collaborations that have been created with specific goals (goal-oriented PPPs)[12] in mind, such as raising awareness in individual Member States.

Third, the risks associated with the lack of a robust cybersecurity infrastructure are cross-cutting and potentially destructive for many sectors of the European economy. This is because the digitalisation of production processes and the use of technology within the service sector can potentially expose the entire digital structure to significant shocks. Moreover, increasing the level of network security within the European digital system is essential due to the imbalance in reactive capability in response to widespread cyber-attacks, since "[...] *within the critical sectors, there are significant differences regarding the maturity level of cyber security. Therefore, some of the critical infrastructure operators will not be as ready as others* [...]".[13] It may also happen that a country recognises the risks to a specific sector or industry from cyber threats but is unable to address them.

[9] "Usually, there are many services that this type of institution delivers, such as research, analysis, development of good practices and guidelines, help desk, security audits and some more focused services," European Union Agency for Cybersecurity (ENISA), "Information Sharing and Analysis Centres (ISACs). Cooperative models", 2018, p. 21-23.

[10] European Commission, The EU budget powering the recovery plan for Europe, COM2020/442 final, 27 May 2020, p. 12.

[11] European Parliament, Regulation of The European Parliament and of The Council, "Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres", COM(2018) 630 final, September 2018, p. 4.

[12] ENISA, Public Private Partnerships..., pp. 24-27.

[13] European Union Agency for Cybersecurity (ENISA), Stock taking of information security training needs in critical sectors, 2017.

In this case, partnerships may be established which aim to identify private organisations where certain tasks can be outsourced, such as creating awareness or supporting the government in its implementation of infrastructure protection measures. 'Hybrid PPPs' have also been defined as a combination of both institutional and outsourced cybersecurity services, applicable in cases where a government "[…] *does not have enough resources to deliver necessary cybersecurity solutions on a national level and starts cooperation with the private entity which has the appropriate expertise and can deliver these solutions.*"[14]

> partnerships may be established aiming at creating awareness or supporting the government in its implementation of infrastructure protection measures.

Before describing the effectiveness of initiatives and partnerships between the public and private sectors, it is necessary to consider how European institutions aim at advancing the whole cybersecurity system, in terms of both cooperation and resilience.

Discussing partnerships in the field of cybersecurity, one must consider the state of uniformity within various infrastructures at the EU level. That is, it is necessary for these infrastructures to pass through regulation, through which the Institutions aim at standardising effective European cybersecurity. Although the European framework regarding cybersecurity still does not seem to be complete, especially with regard to public-private partnerships—even more so in the way that European guidelines are transposed into national legislation[15]—it is important to highlight some general developments to better understand the direction in which European cybersecurity is heading.

One of the most important achievements to date is the Cybersecurity Act.[16] With this regulation, the European Commission demanded the creation of a European regulatory background, the *Common Criteria based European candidate cybersecurity certification scheme* (EUCC), recognised by all Member States. Such a framework should operate according to specific requirements and evaluation standards. The EUCC is based on the Common Criteria for IT Security Evaluation (CC) and the Common Methodology for IT Security Evaluation (CEM). It takes into account the respective standards (ISO/IEC 15408 and ISO/IEC 18045) with appropriate revisions made.[17]

As already described, an important issue when considering the possibility of sharing cooperative projects in cybersecurity at a European level is the evaluation of cybersecurity infrastructural development across Member States.

[14] Ibid., pp. 28-29.
[15] European Court of Auditors, Challenges to effective EU cybersecurity policy, March 2019.
[16] European Parliament, Regulation… "on ENISA…", Art. 48.
[17] European Union Agency for Cybersecurity (ENISA), "Cybersecurity Certification: EUCC Candidate Scheme" v.1.0, 2 July 2020, pp. 15-27.
See also Common Criteria, Common Methodology for IT Security Evaluation.

A “multi-speed cybersecurity” creates, from a strategic point of view, problems in a shared ecosystem because of the difficulty in coordinating different response capacities. Moreover, this could have an impact on the industrial ecosystem, especially among SMEs, which are more exposed to threats due to their inability to bear the costs of cybersecurity.[18] For the purpose of adapting cyber infrastructure to emerging threats, the Network and Information Security (NIS) Directive[19] requires Member States to create National Strategies for Cybersecurity (NCSs), consisting of “[*a*] *high-level top-down approach to cybersecurity that establishes a range of national objectives and priorities that should be achieved in a specific timeframe*”.[20]

> A “multi-speed cybersecurity” creates, from a strategic point of view, problems in a shared ecosystem because of the difficulty in coordinating different response capacities.

Finally, the agreement[21] on public-private partnerships concluded by the European Commission in 2016 with the European Cybersecurity Organisation (ECSO)[22] is an example of cooperation in which the recent legislative improvements described above can be applied. Specifically, in the general framework of Horizon 2020,[23] the necessity to foster cooperation with the private sector in the field of cybersecurity was highlighted. ECSO aims at the better implementation of research within the European digital market, the facilitation of projects by start-ups and SMEs, and ensuring the enforcement of existing security standards.[24] Based on the experiences of such cooperation, as highlighted in the documents published in December 2020, the public sector can work to strengthen investments in the private sector.[25]

In the current framework, any evaluation of a public-private cooperation project in cybersecurity should also take into account the main existing standards and best practices regarding software security,[26] which, in addition to the EUCC, could overcome the problem many organisations face in evaluating the actual security of the software they

[18] K. Kertysova, E. Frinking, K. Dool, A. Maričić, and K. Bhattacharyya, Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks, The European Economic and Social Committee (EESC), 2018, pp. 88-89.

[19] European Parliament, Directive of the European Parliament and of the Council, “Concerning measures for a high common level of security of network and information systems across the Union”, NIS Directive (EU) 2016/1148, 2016.
At the time of publishing, a legislative revision of the Directive, including an impact assessment and Article 114 TFEU, has been scheduled by the Commission for Q4 2020. See also “New initiatives” from the European Commission.

[20] P. Kyranoudi and A. Sarri, Good Practices In Innovation On Cybersecurity Under The National Cyber Security Strategies, ENISA, 2019.

[21] European Cyber Security Organisation (ECSO), “Contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial research and innovation”, Strasbourg, 5 July 2016.

[22] The ECSO was created in order to act as the Commission’s counterpart in a contractual public-private partnership covering Horizon 2020 from 2016 to 2020. The majority of the 250 ECSO members belong either to the cybersecurity industry or to research and academic institutions in the field. To a lesser degree, ECSO members also comprise public sector actors and demand-side industries.

[23] From 2014 to 2020, Horizon 2020 (H2020) was the biggest EU Research and Innovation programme ever.

[24] ECSO, “Contractual arrangement setting up a public-private partnership...”, p. 3.

[25] European Commission, High Representative of the Union, Joint Communication to the European Parliament and the Council, The EU’s Cybersecurity Strategy for the Digital Decade, JOIN(2020)18, 16 December 2020.

[26] There are many recognised standards for software security specifically: ISO/IEC 27034 (one of the most detailed); ISA 99 / IEC 62443 (aimed at IACSs security); PCI SSC (for the certification of payment applications); Microsoft SDL (offering a complete framework for the software development cycle); and ISO/IEC 62304 (specific to medical devices).

use in a complex environment.[27] Mainly this is due to not being able to rely on in-house experts, who may or may not be capable of evaluating the weaknesses of the software in use. In fact, according to an ENISA report, on average, only a small number of technical experts within European industries are able to deeply evaluate such weaknesses. By applying these standards and best practices, the reliability and credibility of security systems can be increased.

The projects of European institutions aim at setting tight standards to increase levels of (cyber)security. The possibility to achieve these results quickly could be fostered by implementing cPPP projects at the European level. There could be advantages for those who take part in these projects: they could rely on recognised standards to certify products—no matter their origin—within the partnership, thus promoting further assurance of the project's quality and reliability. Still, it is difficult to say that this would result in a reduction of risks that may arise in terms of shared responsibility in strategic sectors, as the problem of unwillingness to shoulder them may persist.[28] It is certain that the legislative advancements and recent proposals that have now been put in place could favour some standards in response to possible threats, while increasing importance is given to private sector consultation in drafting the proposals themselves.[29]

Cyber-PPPs to promote the internal market, achieving cyber sovereignty

One of the most highlighted aspects of the recent development of European-level digital infrastructure is that of a Digital Single Market, i.e., efforts to strengthen an internal digital market. This is also crucial for achieving cyber sovereignty in Europe.[30] To reach this stage of independence for the entire European ecosystem, particular attention has been paid to developing a European cybersecurity market. This would also strengthen the European market, permitting the deployment of cross-border services inside the European Union and creating fair competition within the (internal) cybersecurity industry.

These prerogatives must be combined with an examination of the industrial context and the specific characteristics of this market. First, it can be perceived that a sufficient number of providers to create a critical mass capable of competing numerically in the cybersecurity market is lacking. Another important asymmetry is the ability of providers to deliver adequate services, especially when SMEs must respond to requests coming from much larger companies. Finally, it should be stressed that "[...] *ICT* [*products are broadly*] *being driven by non-EU suppliers* [*making*] *Europe* [*dependent*] *on 'foreign' developed ICT products and services, the security of which is determined outside the EU and does not necessarily reflect EU requirements*".[31] These characteristics can certainly be mitigated through the promotion of agreements with the (private) production sector of the cyber security industry.

[27] P. Drogkaris, F. Guasconi, R.van der Veer, and M. Valkema, Advancing Software Security in the EU , ENISA, 2019, pp. 10-12.

[28] Jim Q. Chen, "A Framework of Partnership", The Cyber Defense Review 5, No. 1, International Conference on Cyber Conflict, 2019, pp. 15-28

[29] European Commission, Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities, COM(2020)829, 16 December 2020, p. 7.

[30] European Commission, "A Digital Single Market Strategy for Europe" (COM(2015) 192 final), Brussels, 6 May 2015.

[31] European Cyber Security Organisation (ECSO), "European Cybersecurity cPPP – ECS cPPP – Industry Proposal", June 2016, pp. 40-41.

Encouraging the implementation of cPPP projects in a coordinated manner within the European market would allow for concrete objectives to be reached in less time than in a situation of non-partnership

Indeed, encouraging the implementation of cPPP projects in a coordinated manner within the European market would allow for concrete objectives to be reached in less time than in a situation of non-partnership—a situation where all a cybersecurity project's design costs (including the necessary know-how and R&D expenditure) are borne by the individual EU Member States—while allowing the free market the ability to assert itself.[32] In addition to the issue of efficiency, there is a need to continuously strengthen the sector and devote a lot of resources to areas such as research and maintenance. Above all, this would allow preventive action to be taken in limiting risk by proactively managing threats and moving away from the *"current [European] approach of handling cyber-threats in a reactive mode"*.[33] The EC has furthermore identified three main problems related to the EU's cybersecurity capacities:

1. insufficient level of strategic and sustainable coordination and cooperation between industries, cybersecurity research communities, and governments to shield the economy, society, and democracy with leading-edge European cybersecurity solutions;
2. sub-scale investment and limited access to cybersecurity know-how, skills, and facilities across Europe; and
3. too few European cybersecurity research and innovation outcomes translated into marketable solutions and widely deployed across the economy.

In the absence of a well-defined cooperation mechanism for Member States to work together to improve the resilience of large-scale industrial cyber systems,[34] the issue of cPPP seems to be all the more relevant, providing an equivalent solution to the problem in terms of results (i.e., effective security and reliability).

The recent communication of December 2020 for a European Cybersecurity Strategy envisages the creation of Security Operation Centres alongside a Joint Cyber Unit, with the function of acting *"as a virtual and physical platform for cooperation for the different cybersecurity communities in the EU"*.[35] This important initiative would allow the different actors involved in cybersecurity to confront each other and act within a common space at the technical and operational levels. As the document affirms, *"the Unit would act as a backstop where the participants can draw on one another's support and expertise", and would not be "an additional, standalone body"*.[36]

[32] N. Jentzsch, "State-of-the-art of the Economics of Cyber-security and Privacy", IPACSO - Innovation Framework for ICT Security – Deliverable 4.1, 2016, pp. 9-10.
[33] ECSO, "Contractual arrangement setting up a public-private partnership...", p. 42.
[34] European Commission, "Impact Assessment, accompanying the proposal for a regulation [...]: establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres", SWD(2018) 403 final, 12 September 2018.
[35] European Commission, The EU's Cybersecurity Strategy for the Digital Decade, pp. 7-13.
[36] Ibid., p.14.

Much will depend on how these proposals will be transferred from Member States to private actors in future cooperation with them, i.e., the implementation of any agreements or partnerships. Indeed, a cPPP strengthened by pre-defined standards at a European level would have a positive impact on the relationship between the public and private sectors in terms of *information sharing*, further strengthening their cooperation by also avoiding information asymmetries.[37] Yet it is the very ability to easily share information between sectors (i.e., public and private) that has in fact been identified as a weakness of the EU's cybersecurity strategy.[38] In the case of PPPs, this problem would essentially be overcome, thanks to specific contracts and the early evaluation of projects allowing the parties to focus their efforts on technical questions and common responses to threats.

Cyber-PPP projects carried out in a strategic and coherent way, with a common European framework, and for specific goals, may offer the parties greater guarantees at the design stage, making the whole partnership structures more solid. There is a lot which depends on the interests of individual countries in promoting this type of partnership.[39] This relates to the need for public authorities to be receptive to feedback from the private sector. In fact, private entities have greater knowledge of their specific sectors, and this is an advantage; in the case of cPPPs, this translates to the better protection of the infrastructure to which those entities belong.

> A cPPP strengthened by pre-defined standards at a European level would have a positive impact on the relationship between the public and private sectors in term of information sharing

[37] N. Jentzsch, pp. 21-22.
[38] European Commission, "Assessment of the EU 2013 Cybersecurity Strategy", SWD(2017) 295 final, 13 September 2017.
[39] ENISA, "Information Sharing and Analysis Centres...", p. 35.

Conclusions and recommendations

Rapid detection and coordinated response: given the increasing number of threats and the advanced technology of attackers, large-scale events remain difficult to predict, and the speed of any given response will determine the resilience of the system as a whole. Public-private partnerships in the field of European cybersecurity can play a key role in the development of an adequate and harmonised threat response system. In addition, this would foster the emergence of a thriving European cybersecurity industry, fostering the development of a single European market and contributing to the strategic independence and sovereignty of a Digital Europe.

Shared unified approach: the development of a unified monitoring approach to this type of partnership could help smaller companies to enter the market and compete with larger providers. This does not mean creating new regulations but rather institutionalising the access requirements for private partners at a European level, using security standards as an evaluation metric, and fostering fair competition.

Additionally, the existence of a common European system for accessing PPPs in cybersecurity could facilitate a meritocratic competition, within which small, virtuous companies would be able to compete fairly in the implementation of projects (due to their scalability) in a commonly shared infrastructure, favouring the market.

Technology vs. regulations: technological development remains central in the examination of cybersecurity risks, and this advancement follows a parallel path to the regulatory one. There is indeed a gap between the development of new cyber threats and the creation of procedures to strengthen and quickly adapt the system to such new threats. For this reason, it is crucial to consolidate collaborations between private market actors and those in the field of research so that they can follow the latest developments of technologies, offer cutting-edge services, and provide continually updated solutions—which at the same time means remaining competitive on the market. Finally, cooperation with the private sector would encourage a continuous learning process in terms of best practices but also in terms of partnerships. In fact, private actors with greater experience could provide wide-ranging advice to institutions in terms of project operability and inspire smaller companies, as well.

To build common projects that can enhance the resilience of European cybersecurity and effectively achieve strategic independence, it is therefore advisable:

- to create a stable institutional and legal framework for cPPPs, accepted at a European level by all Member States and capable of eliminating the "bias of pessimism" held by certain States that do not want to entrust parts of their network security to private entities;
- to increase political support for medium- and long-term initiatives, especially with regard to protecting strategic and productive areas of individual Member States, which allocate investments that are strategically capable of attracting large companies, but also especially SMEs, in the IT security sector;

- to involve the research and academic sector in designing theoretical cPPP models that can be implemented in an environment that fosters market competition;
- to create scalable projects at the European level that allow small companies and enterprises to compete in the cybersecurity sector;
- to increase operational cooperation between the public and private sectors, based on the experience of PPP agreements;
- to facilitate investment in the sector through a harmonised tax relief system;
- and, finally, it is important to avoid regulatory fragmentation so that the shared European cybersecurity ecosystem can be strengthened.

Comment on Chapter 2

Francesco Cappelletti has provided an interesting chapter which reviews relevant points related to the development of European-level PPPs in the context of cybersecurity. He has reviewed the characteristics of the PPP as governance method and, therefore, the intrinsic characteristics of PPPs in cybersecurity due to the implications for Member States' security.

In this view, the paper focuses on cooperation between the public and private sectors as a stimulus to foster the European market of cybersecurity, following a liberal approach. However, Cappelletti also underlines a step forward in building cPPP projects within the European framework.

> “It would be useful to apply this anlysis at an operational level too, involving stakeholders and European institutions, starting from a bottom-up approach

He develops interesting points on the application of standards and information-sharing in public-private partnerships, "further strengthening their cooperation by also avoiding information asymmetries." However, it would be useful to apply this analysis at an operational level too, involving stakeholders and European institutions, starting from a bottom-up approach and applying a more holistic understanding of cybersecurity as well as new and leading-edge cyber technologies. Indeed, cyber sovereignty in Europe is a point of cohesion in order to strengthen the EU's potential to act independently in the digital sphere and become a unique strategic actor in the realm of security at an international level.

Luigi Martino

List of Abbreviations

CEM	Common Methodology for IT Security Evaluation
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CIIP	Critical Information Infrastructure Protection
cPPP	Cyber-Public-Private Partnership
EC3	European Cybercrime Centre
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EP3R	European Public Private Partnership for Resilience
EPCIP	European Programme for Critical Infrastructure Protection
EUCC	Common Criteria based European candidate cybersecurity certification scheme
EUROPOL	The Union's law enforcement agency, fully operational since 1999
INTERPOL	International Criminal Police Organization
NCS	National Strategy for Cybersecurity
NIS (Directive)	The Directive on security of network and information systems
PPP	Public-Private Partnership
SMEs	Small and Medium Enterprises

Bibliography

I. Aldasoro, C. Borio, M. Drehmann, *"Early warning indicators of banking crises: expanding the family"*, *BIS Quarterly Review*, March 2018.

R. Bossong and B. Wagner, *"A typology of cybersecurity and public-private partnerships in the context of the EU"*, *Crime Law and Social Change 67* (2017).

P. Burger and I. Hawkesworth, *"How to Attain Value for Money: Comparing PPP and Traditional Infrastructure Public Procurement"*, *OECD Journal on Budgeting* (2011).

M. Carr, *"Public-private partnership in national cyber-security strategies"*, *International Affairs* (2016).

H. Carrapico and A. Barriha, *"The EU as a Coherent (Cyber)Security Actor?"*, *JMS 55, no. 6* (2017).

T. Chaudhary, et al., *"Patchwork of confusion: the cybersecurity coordination problem"* (*research paper*), *Journal of Cybersecurity* (August 2018).

J.Q. Chen, *"A Framework of Partnership"*, *The Cyber Defense Review 5, No. 1, International Conference on Cyber Conflict*, 2019.

N. Choucri, S. Madnick, and P. Koepke, *"Institutions for Cyber security: International Responses and Data Sharing Initiative"* (working paper) Cybersecurity Interdisciplinary Systems Laboratory, *Massachusetts Institute of Technology*, August 2016, https://cams.mit.edu/wp-content/uploads/2016-11.pdf.

G. Christou, *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, *Palgrave Macmillan*, London, 2016, ISBN 978-1-137-40052-9.

P. Drogkaris, F. Guasconi, R.van der Veer, and M. Valkema, *"Advancing Software Security in the EU"*, ENISA, 2019, https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework.

M. Dunn Cavelty, *"A Resilient Europe for an Open, Safe and Secure Cyberspace". UI Occasional Papers 23*, December 2013, https://ssrn.com/abstract=2368223.

B. Hämmerli and A. Renda, *"Protecting Critical Infrastructure in the EU", CEPS Task Force Report*, Brussels, 2010, https://www.ceps.eu/ceps-publications/protecting-critical-infrastructure-eu/.

J. Hardoy, *"Breaking Up a Botnet – How Ramnit was Foiled", Microsoft EU Policy Blog*, 22 October 2015, https://blogs.microsoft.com/eupolicy/2015/10/22/breaking-up-a-botnet-how-ramnit-was-foiled/.

K. Irion, *"The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R)", in The Secure Information Society, eds. J. Krüger, B. Nickolay, S. Gaycken*, Springer, London, 2013.

N. Jentzsch, *"State-of-the-art of the Economics of Cyber-security and Privacy", IPACSO - Innovation Framework for ICT Security* - Deliverable 4.1, 2016.

K. Kertysova, E. Frinking, K. Dool, A. Maričić, and K. Bhattacharyya, *"Cybersecurity: Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks", The European Economic and Social Committee* (*EESC*), 2018, https://www.thehaguesecuritydelta.com/media/com_hsd/report/191/document/qe-01-18-515-en-n.pdf.

E-H Klijn and G.R. Teisman, *"Governing Public Private Partnerships", in Public Private Partnerships: theory and practice in international perspective, ed. S.P. Osborne, Routledge*, London, 2000.

J. Korte, *"Mitigating cyber risks through information sharing", Journal of Payments Strategy & Systems 11, no. 3*, Fall 2017.

P. Kyranoudi and A. Sarri, *"Good Practices In Innovation On Cybersecurity Under The National Cyber Security Strategies", ENISA, 2019, ISBN 978-92-9204-308-7.*

H. Martin, *"Advisory Facility, Value-for-Money Analysis- Practices and Challenges"*, World Bank Institute, 28 May 2013, https://www.icafrica.org/fileadmin/documents/Knowledge/World_Bank/VFM-PPPs-World_Bank-PPIAF.pdf.

R.E. Matland, *"Synthesizing the Implementation Literature: The Ambiguity-Conflict Model of Policy Implementation", Journal of Public Administration Research and Theory no. 5*, April 1995.

A. Mermoud et al., *"To share or not to share: a behavioral perspective on human participation in security information sharing", Journal of Cybersecurity 5, no. 1*, June 2019.

C. Osborne, *"Police, security firms team up and take down Skylock malware", ZDnet*, 11 July 2014, https://www.zdnet.com/article/police-security-firms-team-up-and-take-down-shylock-malware/.

E. Ouzounis, *"PPP and ISAC in the EU" presentation*, Attiki, 14 December 2018, https://www.oecd.org/internet/global-forum-digital-security/events/gfdsp-dec2018-ouzounis.pdf.

S. Piattoni, *"Multi-level Governance in the EU. Does it Work?", Globalization and Politics – A Conference in Honor of Suzanne Berger,* Massachusetts Institute of Technology, May 2009.

S. Purser, *"The European cooperative approach to securing critical information infrastructure", Journal of Business Continuity & Emergence Planning 5, no. 3,* Fall 2011.

C. Pursiainen, P. Gattinesi, *"Towards Testing Critical Infrastructure Resilience", JRC Scientific and Policy Reports,* 2014, https://core.ac.uk/download/pdf/38627770.pdf.

A. Rotondo, *"Cybersecurity e protezione delle infrastrutture critiche: l'efficacia del modello europeo", in Lo spazio cyber e cosmico: risorse dual use per il sistema Italia in Europa, eds. S. Marchisio and U. Montuoro, Giappichelli Editore,* Turin, 2019.

R. Setola, E. Luiijf, and M. Theocharidou, *"Critical Infrastructures, Protection and Resilience", in Managing the Complexity of Critical Infrastructures. A Modelling and Simulation Approach, eds. R. Setola, V. Rosato, E. Kyriakides, and E. Rome,* Springer, Berlin, 2016.

P. Timmers, *"The European Union's cybersecurity industrial policy", Journal of Cyber Policy 3, no. 3,* November 2018.

Other sources

Common Criteria, *Common Methodology for IT Security Evaluation,* April 2017, https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf.

Cuncil of the European Union, Council Resolution of 18 December 2009 on a Collaborative European Approach to Network and Information Security, (2009/C 321/01), 29 December 2009, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF.

Council, "Shaping Europe's Digital Future", Brussels, 9 June 2020, https://data.consilium.europa.eu/doc/document/ST-8711-2020-INIT/en/pdf.

European Commission, "Assessment of the EU 2013 Cybersecurity Strategy", SWD(2017) 295 final, 13 September 2017, https://ec.europa.eu/transparency/regdoc/rep/other/SWD-2017-295-F1-EN-0-0.PDF.

EC, *Commission Staff Working Document on the Review of the EPCIP,* SWD(2012) 190 final, 22 June 2012, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/policies/crisis_and_terrorism/epcip_swd_2012_190_final.pdf.

EC, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786, 12 December 2006, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:EN:PDF.

EC, "A Digital Single Market Strategy for Europe", (COM(2015) 192 final, Brussels, 6 May 2015, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN.

EC, The EU budget powering the recovery plan for Europe, COM2020/442 final, 27 May 2020, https://eur-lex.europa.eu/resource.html?uri=cellar:4524c01c-a0e6-11ea-9d2d 01aa75ed71a1.0003.02/DOC_1&format=PDF.

EC, European Cyber Security Organisation, Contractual arrangement setting up a public-private partnership in the area of cybersecurity industrial research and innovation between the European Union and the European Cyber Security Organisation, Strasbourg, 5 July 2016, https://ecs-org.eu/documents/contract.pdf.

EC, *Green Paper on a European Programme for Critical Infrastructure Protection,* COM(2005) 576, 17 November 2005, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005DC0576.

EC, "Impact Assessment, accompanying the proposal for a regulation [...]: establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres", SWD(2018) 403 final, 12 September 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:0403:FIN.

EC, High Representative of the Union, Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020)18, 16 December 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164.

EC, High Representative of the Union, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1, 7 February 2013, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001.

EC, Network and Information Security: Proposal for A European Policy Approach, COM(2001) 298 (6 June 2001), https://ec.europa.eu/transparency/regdoc/rep/1/2001/EN/1-2001-298-EN-F1-1.Pdf.

EC, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48, 7 February 2013, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013PC0048.

EC, Proposal for a Directive of the European Parliament and the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148, COM(2020)823, 16 December 2020, https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union.

EC, Proposal for a Directive of the European Parliament and the Council on the resilience of critical entities, COM(2020)829, 16 December 2020, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf.

EC, "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", SEC(2009) 399, 30 March 2009, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52009DC0149.

EC, Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry, COM(2016) 410, 5 July 2016, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16546.

European Court of Auditors, *Challenges to effective EU cybersecurity policy,* March 2019, https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=49416.

European Cyber Security Organisation, "Cybersecurity in Light of Covid-19" Report, 2020, https://www.ecs-org.eu/documents/uploads/report-on-the-ecso-members-and-the-community-survey.pdf.

European Cyber Security Organisation, "European Cybersecurity cPPP – ECS cPPP – Industry Proposal", June 2016, https://ecs-org.eu/documents/ecs-cppp-industry-proposal.pdf.

European Parliament, Directive of the European Parliament and of the Council "Concerning measures for a high common level of security of network and information systems across the Union", NIS Directive (EU) 2016/1148, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A32016L1148.

EP, Regulation of The European Parliament and of The Council "Establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres", COM(2018) 630 final, September 2018, https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-centres-regulation-630_en.pdf.

EP, Regulation of The European Parliament and of The Council "on ENISA and on information and communications technology cybersecurity certification [...] - Cybersecurity Act", EU 2019/881, 17 April 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=en.

European Union Agency for Cybersecurity, " Cybersecurity Certification: EUCC Candidate Scheme" v.1.0, 2 July 2020, https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme/.

ENISA, *EP3R 2009-2013 Future of NIS Public Private Cooperation,* 2015, https://www.enisa.europa.eu/publications/ep3r-2009-2013.

ENISA, "Information Sharing and Analysis Centres (ISACs). Cooperative models", 2018, https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models.

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

ENISA, *Stock taking of information security training needs in critical sectors,* 2017, https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors/at_download/fullReport.

United Nations Office of Counter-Terrorism and United Nations Counter-Terrorism Committee Executive Directorate, *The protection of critical infrastructures against terrorist attacks: Compendium of good practices,* 2018, https://unrcca.unmissions.org/sites/default/files/eng_compendium-cip-final-version-120618_new_fonts_18_june_2018_optimized.pdf.

United States Government, "Critical Infrastructure Protection Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism)", 2001, https://www.law.cornell.edu/uscode/text/42/5195c.

EUROPEAN LIBERAL FORUM

Scan for other ELF Discussion Papers

Contacts: +32 (0)2 669 13 18 // info@liberalforum.eu // **www.liberalforum.eu**