Francesca Castaldo and Federico Serini

Public-private collaboration in European cybersecurity. Between organizational and regulatory plans[*]

Abstract: Bringing together considerations straddling organizational business science and public law, the paper aims to provide a multidisciplinary overview of public-private collaboration in the context of cybersecurity. Two profiles are analysed: the public-private partnership, an organizational and legal perspective, and the phenomenon of co-regulation in cyber security technical standardization and certification. The study of the two profiles just mentioned will allow us to analyse the role of private parties, in one case as recipients of the cybersecurity obligations of secondary legislation then translated at the national level, and on the other as actors who promote and participate in the elaboration of technical cyber security standards. The opportunity is to contextualize said phenomenon, as well as to grasp its ongoing evolutionary profiles and criticalities.

Keywords: Cybersecurity; Public and private power; Technical regulation; Public-private partnership; Strategic alliances.

1. Introduction

The legal debate on the governance of cyberspace[1], the well-known interest of States in regulating and controlling this new and unprecedented space that has the characteristic of being a "non-territory", can be generally interpreted as a test of State sovereignty in the globalization time. Indeed, cyberspace represents

* This paper results from a joint reflection by the Authors. However, §§ 2 and 3 are attributable to Francesca Castaldo, while §§ 4 and 5 are attributable to Federico Serini. The introduction in § 1 and the conclusions in § 6 are the product of considerations by both Authors.

1 By cyberspace we mean an agglomeration of products, processes, and services pertaining to information and communication technologies (henceforth "ICT goods") circulating in the global marketplace, which, at the level of services, includes the Internet. On this point may it be granted to refer to Serini 2023a.

Teoria e Critica della Regolazione Sociale, n. 2, 2024 • Mimesis Edizioni, Milano-Udine Web: www.mimesisjournals.com/ojs/index.php/tcrs • ISSN (online): 1970-5476 • ISBN: 9791222320786 • DOI: 10.7413/197054760154

a challenge for the public powers that have always been tied to the material element of territoriality[2].

Curious, however, is the genesis of this dimension. Cyberspace was originally a public phenomenon, born with Arpanet project (the prototype of today's network of networks, i.e., the Internet), but later developed and spread through private individuals and outside the States' control[3].

The entry of information technology into the market and society[4] has been an event of little interest to public power[5], which has limited itself to intervening with regulations aimed rather at favouring the economy and investment in this sector, as well as the regulation of the mechanisms of technical operation of the network[6], without ever being interested in intervening in the "political" side of cyberspace[7].

After this initial period of indifference, the increasing social and economic relevance of this environment, caused by the negative consequences arising from cyber-attacks and information technology malfunctions, have led public authorities to turn their attention to this space, demonstrating "not only that they [can] regulate it but also that they 'hyper-regulate'"[8].

The question before us today is how government intervention – successive in time – intends to regulate cyberspace, now understood as a space regulated primarily by forms of self-regulation, first by users themselves, then by large private groups.

In addition to the creation, over time, of an *ad hoc* administrative organization[9], empirical evidence shows that in this dimension it is usual to witness forms of so-called multistakeholder governance, where States are placed on the same level as other actors, often private (i.e. see the Internet regulation)[10].

The framework of security policies, as a typical expression of public sovereignty, in cyberspace, seemed to be a privileged vantage point for analysing the relationship between powers in the digital and reflecting on the peculiar traits of that cooperation between public and private power, which is its essence in this area.

2 Irti, 2006: 4.

3 Bombelli 2017: 26.

4 Heritier 2003.

5 Della Morte 2018: 27.

6 The reference is first of all to the codes, programs and protocols that underlie the functioning of communication in cyberspace, on which point see L. Lessig 1999, where the A. writes «[l]ife in cyberspace is regulated primarily through the code of cyberspace» (p. 83), but also to the centralized management of interconnection standards and the DNS system of domain names, which is delegated to the U.S.-based Internet Corporation for Assigned Names and Numbers-ICANN, governed by a structure in which government representatives, technical organizations, and private companies sit.

7 One is reminded of the rich debate in the early 1990s of the last centuries, animated by criticisms concerning not only the profiles of feasibility, but also the appropriateness and legitimacy of a legal regulation of this "new space". On the point s. Pollicino, Bassini, De Gregorio 2022: 4 ss.

8 Pollicino 2023: 415.

9 On this point, about the Italian and European legal systems, we refer to the work of Rossa 2023.

10 Cerf 2022: 7 ss.

Starting from these brief premises, this paper intends to investigate such collaboration from a multidisciplinary perspective between legal and corporate organizational sciences, according to the academic interests of the authors.

After an initial reflection on the role of private individuals in (cyber)security (§2), the reflection continues by focusing on the transversality of the forms of collaboration, or alliances, public-private for countering cyber threats (§3) arguing on the peculiar and fundamental role assumed by public-private partnerships (PPPs) in cybersecurity from an organizational perspective (§4). as well as subsequently, from the Public Law point of view, on the relevance of standard-setting bodies and technical standardization in this area, as instruments of private origin lent for the regulation of public interests such as security (§ 5). The discussion of these topics will finally allow us to draw some final considerations that refer to the broader question of the relationship between public and private power (§ 6).

2. Private participation in cybersecurity

According to sociological sciences, the globalization process has led to a rearticulation of the State that has effectively transferred some of its functions to private actors[11], including, over time, security[12].

From the legal perspective, this has resulted in a progressive distinction between roles and functions belonging to public (or primary) security, which is made explicit in the exercise of authoritative and repressive powers, and forms of secondary or subsidiary security (itself distinguished into "complementary" and "community" security) where private entities also participate to complement, aid or supplement the police function[13].

In the Italian legal system, the latter securitarian meaning has been made possible by the principle of subsidiarity in Article 118(4) of the Constitution, which opens citizens as well as economic activities to the performance of activities in the general interest, which includes security[14].

At the European level, this openness has been possible on the back of a series of pronouncements since the 1970s by the Court of Justice on the relationship between the activities of public authorities and the framework of European economic freedoms.

The Court has been called upon to resolve questions arising from the conflict between the conditions to which States subject the exercise of private security functions such as citizenship, possession of a license, taking an oath, administrative setting of fees as forms of control and surveillance to which such activities are subjected by the public power of States, with the right of establishment of workers in the European space.

11 Sassen 2008.
12 Abrahamsen 2016.
13 Mosca 2012: 26; Aliquò 2023.
14 Ursi 2022: 204 ss.

With these decisions, the European Court has interpretatively extended European integration in this area, denying that the intervention of private parties in functions of traditional State prerogative should automatically qualify as the exercise of a public power over which market freedoms cannot take effect since the issue must be assessed on a case-by-case basis[15].

In cybersecurity, however, we see a further phenomenon than the one just mentioned of "privatization of security", that is, relating to the involvement of entities that carry out private security activities. Indeed, in this sector, we find the involvement of private organizations that have nothing to do with security in the traditional sense although they are now largely involved in it[16].

One thinks of the various critical infrastructures operating in the sectors of relevance to the society and economy of the states subject to the European NIS framework and, as far as Italy is concerned, falling within the *Perimetro di Sicurezza Nazionale Cibernetica* (PSNC), which are called upon to have to actively participate in the national cybersecurity process as well as the European one.

In other cases, this involvement finds expression in forms of collaboration embodied in public-private partnerships (see §4) that are useful both for countering cybercrime (this is the case with the various information-sharing ecosystems between public authorities and critical)[17], both for technology transfer between universities and industry[18].

3. Facing the cyber threat: the need for alliances

It is widely acknowledged that the cyber threat is multifaceted and diverse. Despite the common perception of cyber-attacks as originating from an invisible enemy, they can be categorized into various types, including malware (viruses, worms, Trojans), phishing, DDoS (Distributed Denial of Service) attacks, ransomware, and social engineering attacks, among others.

The motives behind such attacks are also very diverse, ranging from simple espionage, aimed at gathering sensitive information from governments, companies or individuals, to hacktivism motivated by political or social ideologies; from cybercrime motivated by financial gain, as in the case of ransomware or the theft of banking information, to all-out cyber warfare, with state-sponsored attacks aimed at gathering strategic information or sabotaging critical infrastructure[19].

15 Buzzacchi 2015: 114 ss.

16 Farrand, Carrapico 2018: 197-217.

17 Let it be permissible to refer to F. Serini 2023b, 2024.

18 Reference is made to the European Digital Innovation Hubs (EDIHs), whose aim is to ensure the digital transition of industry, particularly small and medium-sized enterprises (SMEs), and the public administration through the adoption of advanced digital technologies such as artificial intelligence, high-performance computing, and cybersecurity.

19 Castaldo 2019; Eckert 2005.

Cyber-attacks can also hit different targets: critical infrastructure such as power grids, communication systems and other vital infrastructure, a bank, a hospital or a local authority, to name but a few.

The use of botnets and automated scripts to launch large-scale attacks, combined with the ubiquity of Internet connectivity, allows the threat to spread rapidly across global networks.

Furthermore, the use of evasion techniques by hackers, such as encryption or code obfuscation, to mask their activities and evade detection, and the use of anonymity tools and proxies to conceal the origin of attacks, demonstrates why the problem of attribution is so relevant in the cyber sphere.

The cyber threat is, therefore, not only asymmetrical in military terms but also has the potential to cause significant economic damage (loss of data, service interruptions, recovery and compensation costs), operational disruption (interruption of business operations, loss of productivity) and reputational harm (damage to the reputation of affected companies or entities)[20].

The impact of cyber threats extends beyond mere productivity losses. Reputational damage, national security concerns, and the necessity to adapt to the continuous evolution of technology and develop new defence strategies are also significant considerations[21].

In light of the aforementioned considerations, addressing this pernicious threat is a formidable challenge for all stakeholders, public and private, who are unable to ignore it in their operations[22].

The characteristics mentioned collectively constitute a complex and evolving challenge to the cyber threat, necessitating a state of constant vigilance and the implementation of advanced and adaptable defence strategies.

Although the most sophisticated computer systems are now 'resilient by design'[23], i.e. to be able to guarantee their operability in the event of an attack, i.e. to ensure *business continuity* and *disaster recovery*, we must not forget that the main vulnerability in the cyber universe remains the human one, i.e. linked to the intrinsic weakness of the so-called 'human factor'[24].

Considering the current technological landscape, which presents an ever-increasing number of potential attack vectors, no entity, whether private or public, is currently capable of defending itself effectively and remaining resilient against cyber-attacks.

Consequently, there is a pressing need for collaboration between the public and private sectors, as well as the opportunity to form alliances against the common, invisible adversary[25].

20 Castaldo 2018b.
21 Castaldo 2019; Castaldo and Serini 2024.
22 Castaldo 2018b.
23 Castaldo 2021.
24 *Ibidem*.
25 Castaldo 2018a.

In the contemporary globalized, uncertain and interconnected environment, collaboration has become a necessity to address challenges and seize opportunities[26]. This is particularly pertinent in VUCA (Volatile, Uncertain, Complex, Ambiguous) scenarios, which are often employed to describe the highly complex nature of our world[27].

4. A peculiar form of alliance to counter the cyber threat: public-private partnerships

Cooperation can take the form of a public-private partnership, a type of alliance that is not only tactical, arising in response to a contingent risk, but strategic, i.e. long-term, and therefore perfectly suited to dealing with the cyber threat, given its time horizon.

Public-private partnership is a concept based on the idea of combining the resources, skills and perspectives of the public and private sectors to address common challenges and pursue development opportunities[28].

Public-private partnerships (PPPs) have a long history, dating back several decades. However, in recent years they have become more relevant and widespread globally.

These types of partnerships have emerged primarily as a response to the growing complexity of social and economic challenges and the need to develop innovative models for financing and managing infrastructure and public services[29].

Public-private partnerships are in fact cooperation agreements between a public organization and one or more private companies. The objective of a PPP is to design, finance, build, operate and/or maintain infrastructure or provide public services[30].

This model is widely used in sectors such as transport, energy, health, education and water. In essence, PPPs are organizations in which public bodies and private companies work together to achieve common goals. This form of collaboration leverages the strengths of both the public and private sectors, fostering an environment conducive to innovation, efficiency, and sustainability[31].

Public-private partnerships (PPPs) are rooted in theoretical frameworks from various disciplines, including economics, organizational theory, public finance, and public policy theory.

In economics, PPPs are linked to public goods theory and the concept of public sector inefficiency. It is widely believed that private sector involvement can im-

26 Volpe and Castaldo, 2022; 2024.
27 Castaldo 2023; Zanda and Castaldo, 2023.
28 Broadbent and Laughlin 2005; Hemming 2006.
29 George *et al.*, 2024.
30 Broadbent and Laughlin 2005; Hodge *et al.* 2017.
31 George *et al.*, 2024.

prove efficiency in the delivery of public services, especially in areas where the government faces challenges[32].

Organizational theory emphasizes the potential of the private sector to provide specialized management resources and skills to improve the management and efficiency of public operations[33].

Public policy theory focuses on the responsibility and role of government in addressing social issues and providing public services. From this perspective, PPPs can be analyzed as a form of innovation in public governance that involves private actors in the realization of public objectives[34].

These theories, despite their inherent peculiarities, provide the intellectual basis for understanding the underlying motivations behind the emergence of public-private partnerships.

A substantial body of literature exists in the economic, organizational and financial fields which describes the advantages of these alliances. These advantages typically include access to the partner's complementary resources and skills[35].

One of the main issues addressed in the literature when identifying the benefits of PPPs is that of economic efficiency: some scholars argue that these alliances can lead to greater efficiency in the delivery of public services due to the participation of the private sector[36].

One of the main disadvantages of public-private partnerships is the unequal distribution of risk between the public and private sectors, with the state – according to some theorists – bearing a disproportionate share of the burden[37].

Another much-discussed issue is the complexity of managing the relationship between the public and private sectors, two different worlds with different cultures and therefore a potential source of conflict[38].

Another critical factor is the potential for the short-term financial interests of the private sector to conflict with the long-term goals of the public sector in terms of social welfare and environmental sustainability. This is compounded by the risk of overcharging for privately managed services and infrastructure, which can result from inefficiencies in decision-making or a lack of transparency in private partner selection procedures and/or concession contracts[39].

There is a growing interest in assessing the long-term financial sustainability of public-private partnerships, particularly in light of financial risks and their impact on public finances[40]. It is therefore important to address the challenges that these partnerships present through proper design, monitoring, and evaluation, ensur-

32 Grimsey and Lewis 2007; Hemming 2006, Hodge et al. 2017.
33 Hemming 2006.
34 Osborne and Brown 2005.
35 Castaldo 2018a.
36 Broadbent and Laughlin 2005; Grimsey and Lewis 2007; Hodge *et al.* 2017.
37 Rybnicek, Plakolm and Baumgartner, 2020.
38 Castaldo 2018a.
39 Vining and Boardman 2008.
40 Grimsey and Lewis 2007.

ing a balance between public and private interests and maximizing the benefits to society as a whole[41].

Indeed, there is considerable debate surrounding the efficacy of public-private partnerships in ensuring accountability, oversight, and transparency, particularly in light of the involvement of private actors in the provision of essential public services such as health and education[42].

Given the inherent complexity and coordination required for this form of alliance, it is of the utmost importance that public-private partnerships are designed and managed in a transparent, fair and accountable manner if they are to function effectively.

This necessitates the establishment of a robust legal framework, monitoring and evaluation mechanisms, and apparatus to ensure the protection of public interests and the equitable distribution of benefits and risks among all stakeholders. Consequently, it is of paramount importance to conduct a comprehensive assessment of the potential effects of a public-private partnership on the partners and all stakeholders, as well as the allocation of benefits and risks to each party, prior to the establishment of the partnership[43].

While in other sectors, public-private partnerships are the result of a cost-benefit analysis, in the cyber universe the reality is quite different[44]. Here, the challenge is to combat an imperceptible enemy that lurks menacingly in the so-called 'fifth domain'[45], the 'borderless' space.

As previously stated, the cyber threat is not only multifaceted and unpredictable but also continuously changing in technological terms[46].

In such a volatile, uncertain, complex and ambiguous (VUCA) scenario, no player, public or private, can move cautiously and profitably in the face of the threat of cyber-attacks.

Consequently, there is a need to form alliances to fight an asymmetrical battle against a common, invisible, unscrupulous and powerful enemy[47].

In other words, while in other areas public-private partnerships are the result of a well-considered and mutually beneficial decision, in a typical win-win strategic mode, in the cyber sector we are faced with a necessity, a categorical imperative[48].

It is clear that cyber security concerns affect both the public and private sectors. Therefore, public-private partnerships are the most suitable forum for collaboration between the two sectors to develop collective methods to counter

41 Broadbent and Laughlin 2005; Grimsey and Lewis 2007.
42 Dunn-Cavelty and Suter 2009; George *et al.*, 2024.
43 Broadbent and Laughlin 2005; Hodge *et al.* 2017.
44 Thomas 2013.
45 Per 'quinto dominio' si intende il dominio bellico più recente, che si aggiunge ai quattro noti: terra, acqua, aria e spazio.
46 Castaldo 2019; 2021.
47 Castaldo 2021.
48 Castaldo and Serini, 2024.

cyber threats. Attacks on critical national infrastructures have the potential to cause significant damage to citizens' lives, services, operations and continuity. It is therefore essential that the public and private sectors are protected against cybercriminals with effective and adaptable policies, regulations and strategy implementations.

In this context, public-private partnerships represent an organizational effort to protect the common interests of prevention, security and the creation of secure environments.

The issue of cyber security threats is a global problem, which was recognized by the EU and its individual institutions relatively early on. It was agreed that this problem can only be addressed through equally 'global' responses, requiring international communication, harmonized legislation and efforts from both the public and private sectors.

However, cybersecurity issues are complex in nature, which sometimes makes a unified approach difficult to achieve[49].

In order to address this difficulty, the European Commission published a communication in 2001 entitled "Europe's Transition to the Information Society". This communication proposed several actions to protect information and communication infrastructures. It called for the implementation of a comprehensive policy initiative, the establishment of a unified definition of cybercrime, enhanced communication with stakeholders, and increased funding for research and development to address these threats. Since that time, now more than two decades ago, and more intensively in the last decade, there have been several successful PPP models, just as there has certainly been no shortage of failures. Nevertheless, these alliance attempts will continue to be implemented, following the rapidly developing developments in 'attacker' technology[50].

It is only by forming alliances and joining forces that public and private entities can collectively defend themselves against the risk of elimination, to build a better and more resilient world in line with the UN Agenda[51]. The 17th and final Sustainable Development Goal (SDG) for 2030 is 'Partnerships for the Goals'. This identifies partnerships as the optimal means of addressing the challenges facing humanity and the planet as a whole[52].

In conclusion, public-private partnerships represent a powerful tool for addressing the complex and interconnected challenges facing the world today[53]. By fostering a shared commitment and effective collaboration between the public and private sectors, we can achieve significant and lasting results for the common good of our society and our planet.

49 Castaldo 2018b.
50 Laughlin 2015.
51 Castaldo, Porretta and Zanda, 2024.
52 Eweje *et al.*, 2021.
53 Laughlin 2015.

5. The relevance of entities and technical standards in cyber resilience

The cases just mentioned refer to forms of cooperation and collaboration directed toward ensuring cybersecurity in the narrow sense, that is, responding to threats that may pose dangers and, thus certain damage.

Action other than cyber resilience, as a form of security that best fits the needs of the risk society, where harm is a future event, probable and not certain.

Resilience focuses on prevention from threats and minimisation of the effects resulting from the realization of the threat (damage) with an approach that starts from accepting the failure of security measures by providing for mitigation and damage mitigation measures so that the system continues to exist, and its collapse is averted[54].

This is where technical security standards for both products and processes come in since these tools make it possible to make risk calculable (in this case cyber[55]).

These are tools that do not have a legal nature since they are not the result of a legal-political process within Parliaments but are produced within alternative centres of interest aggregation – standard organizations (SO) – which see the participation of both States but also, and above all, of the various private stakeholders operating in the area of interest.

SOs are entities, often private, responsible for producing technical standards. They operate in the multilevel and, for essential historical reasons there are no more than three: one for the electronics sector, one for the telecommunications sector, and one for all other sectors[56].

At the international level, there are the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU). At the European level, we find the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI). In Italy, the recognized bodies are the Ente Nazionale Italiano di Unificazione (UNI) and the Comitato Elettrotecnico Italiano (CEI).

A relationship exists between technical regulations and the legal system[57], according to which the technical standard acquires relevance for the legal system whenever it is "assumed" within it, and this occurs through the institutes of incorporation and referral. There is incorporation when the content of the technical standard is transposed *sic et sempliciter* within a legal source (usually primary and/or secondary), while referral consists in the explicit reference to a technical standard punctually indicated (fixed or material referral), or in the use of general clauses within a legal provision, such as the reference "to the best available techniques", "to the state of the art", or rather to the "best standards. technical and

54 Bourdeau 2013; Dunn Cavelty, Eriksen and Scharte 2023.
55 Oddenino 2018.
56 Elias 1995: 32.
57 Bombelli 2023: 1-14.

safety standards", referring to compliance with technical regulations as a prerequisite of good practice (mobile or formal referral)[58].

In cybersecurity regulation, the link between technical and legal standards is a characteristic feature that we can already grasp from the definition provided by the European legislator with Regulation (EU) 2019/881 (Cybersecurity Act). Indeed, with this act, the Union introduced – for the first time within a legal norm – the notion of cybersecurity, defining it in Article 2(1) as "the set of activities necessary to protect the network and information systems, the users of those systems and other persons affected by cyber threats".

This formulation not only introduced into the (European) legal system a concept previously relegated to the exclusive domain of technicians but also gave it social and political value.

This can be grasped from the fact that in the first part, the reference to "protection of the network and information systems" can be interpreted as a form of (moving) reference to the confidentiality, integrity and availability (so-called RID) of information and the medium that contains it, as a fundamental feature of information and computer security, already originally defined in the first technical standards in the field between the '80s and '90s[59].

However, is in the second part that we find the innovative feature of this definition, namely the reference to the "security of the human" understood not only as the user, but also as any individual who can be negatively impacted by information technology, or threats conveyed through it.

We believe that with this formulation, the European Union has directed cybersecurity toward the public purpose of protecting individuals beyond the security of the single market and has done so by directing the purpose of industry technical standards, usually directed toward the exclusive protection of the individual organization so that its business is preserved[60].

We find confirmation of this in the document "An EU strategy on standardization Defining global standards in support of a resilient, green and digital EU single market" published by the European Commission in February 2022[61], where the Commission noted that "[o]rder than ever, standards cannot be limited to dealing only with technical components, but must also integrate fundamental democratic values and EU interests as well as ecological and social principles",

58 Greco 1999: 37 ss.

59 Russel, Gangemi 1991: 23. In particular, for the history of the technical standard ISO/IEC 27001, refer to Gallotti 2022: 247 ss.

60 In the ISO/IEC 27001:2013 standard for information security management systems, the definition of an "Information security incident" was "Single or series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security". The recently updated version of the standard, revised considering legislative interventions in the areas of personal data protection and cybersecurity, now defines the concept as "one or multiple related and identified information security event that can harm an organization's assets or compromise its operations".

61 Communication, An EU strategy on standardization: Setting global standards in support of a resilient, green, and digital EU single market, COM (2022) 31 final, 2.2.2022.

and also specifically referred to the "strategic dimension" of technical standards on cybersecurity or critical infrastructure resilience, thus deeming it appropriate for the European standardization system-composed of the three private and independent bodies CEN, CENELEC and ETSI to respect and promote European values and interests[62].

The theme is thus relatable to the broader reflection on the relationship between public and private power at this juncture.

A gradual convergence of the technical standardization system towards compliance with principles with a Public Law vocation has been observed for some time, without going through the "juridicization" of the technical standard or the "publicization" of the bodies that produce said standards, which therefore remain private.

The standardization process at these bodies takes place by the principles dictated by the World Trade Organization (WTO) in 2000[63], namely: coherence (standards cover different technical disciplines, coherence and cohesion between them must be ensured), transparency and openness (all proposed standards and draft standards are made public for comments before the final version is published. Any objection must be discussed with the person who raised it), consensus (the content of standards is defined based on mutual agreement), voluntary application (standards are not mandatory), independence from special interests, and efficiency.

However, although these principles give hope that the process of forming these rules, which are non-legal and produced by entities of a private nature, will be guided by considerations and models of jurisprudential inspiration, the doctrine has had to point out some critical aspects, especially concerning the aspect of participation of social representations, as well as the different weight of certain subjects in voting, which would leave one leaning toward industrial representations[64].

It is worth pointing out, however, that as is evident from the analysis of European strategy documents, the Union's interest is placed on a particular type of technical standard, which is the harmonized standard.

According to Article 2(1)(c) of Regulation 1025/2012 on European standardization, a harmonized standard is "a European standard adopted based on a request from the Commission to apply Union legislation on harmonization", the formation procedure for which is detailed in Article 10 of the same Regulation.

Unlike other technical standards, harmonized standards are not created at the behest of different interest groups but are formulated by the European standards organizations (CEN, CENELEC and ETSI) at the request of the European Commission. The three European bodies can also refuse to comply with that request but, if they accept, they are obliged to respect the content and constraints con-

62 *Ivi*: 4.

63 These are six principles agreed upon by the TBT Committee in 2000, aimed at guiding Members in the development of standardization processes. They can be found on the official WTO page at the following link.:<https://www.wto.org/ english/tratop_e/tbt_e/principles_standards_tbt_e.htm>.

64 Hachez, Wouters 2011: 677-710.

tained therein. The Commission also reserves the right to exercise extensive power of control over these bodies, both during the formulation phase of the standard and during its approval[65].

Given the private nature of the SO and the role of the Commission in the process of forming these standards, usually, the harmonized standard is an example of public-private co-regulatory[66].

These standards will have an increasing importance in the digital policies of the European Union.

In the 2024 version of the Rolling Plan for ICT standardization, the annual document in which the state of the art of ICT standardization activities in the European context is represented, it is envisaged that after the adoption of the proposed Regulation (EU) 2022/272 (also known as the Cyber Resilience Act – CRA), the European Commission will prepare a formal standardization request to support the implementation of the CRA.

The figure is of particular significance because it highlights the Union's strong preference for using this type of technical standard, as opposed to others, in the context of digital technologies.

This, however, led the European legislature to have to intervene in the matter in 2022 by making important changes to Regulation 1025/2012 first and foremost by promoting and encouraging the participation of social representations within the three European bodies[67]. In addition, a communication of the same year introduced the possibility for the European Commission to adopt common technical specifications using implementing acts to ensure the protection of the public interest in cases where there are no harmonized standards or existing ones are insufficient[68].

The latter power finds expression in certain areas, including those of cybersecurity (by the proposed Cyber Resilience Act Regulation)[69] and Artificial Intelligence[70].

6. Concluding remarks

In a few lines, the contribution aimed to draw an overview of the estimation of the relationship between the public and private sectors in the context of cybersecurity in its transversality.

This collaboration represents an inevitable necessity dictated by the very nature of cyberspace, which we can interpret as an agglomeration of ICT products, processes and services, put on the market by private companies active in the field

65 Art. 10 Reg. (UE) 1025/2012.

66 Kamara 2017.

67 Art. 1, Reg. (UE) 2022/2480.

68 Comunicazione, *Una strategia dell'UE in materia di normazione Definire norme globali a sostegno di un mercato unico dell'UE resiliente, verde e digitale*, COM (2022) 31 final, 2.2.2022.

69 Comunicazione, *Una strategia dell'UE in materia di normazione* cit.: 5-6.

70 Volpato 2024.

and traded according to the laws of supply and demand, as well as respecting the relevant production and quality standards (commodity cyberspace)[71].

This has led to the need to establish such forms of both public and private intervention, which we can grasp from an organizational perspective, see precisely the aforementioned public-private partnerships (PPPs); as well as at the regulatory level, where in the digital context it is not unusual to witness the phenomenon of so-called co-regulation, or multistakeholder governance, in which states are placed on the same level as other actors, mostly private.

The synergy created in these systems thus makes it possible to cope with the cybernetic threat, on the one hand, from an organizational point of view, by pooling the resources, skills and infrastructure of the public administration and private individuals, and on the other hand, from a regulatory point of view, by dictating regulations of a mixed nature between the legal and the technical, capable of expressing a multitude of interests that can be traced mostly to public interests, usually enforced by States, and economic interests, proper to the sectoral industries that participate in technical standardization.

In addition to the benefits, however, the discussion has also had the opportunity to highlight the negative aspects of this relationship, due to difficulties originating from the very nature of the parties involved.

The economic efficiency of PPPs, demonstrated by better delivery of public services, is matched by the unequal distribution of risk between the public and private sectors, with the state-according to some theorists-bearing a disproportionate share of the burden[72].

Consider also the critical issues posed by the potential conflict between the short-term financial interests of the private sector and the long-term goals of the public sector, which could result in an impediment to the achievement of goals in terms of social welfare and environmental sustainability given by the risk of overcharging for privately operated services and infrastructure.

As will be understood, the topic refers to the complex relationship between public and private powers, which we believe can be easily analysed from the normative perspective.

The assertion of private powers in cyberspace is a well-known fact by now (§ 1) what is of interest here, however, is the ability to express one's interests using technical standardization, as an instrument of a private nature, until not so long ago thought to be neutral in that it was produced outside the circuits of political representation.

However, in the European context, we have had to point out that the Union's interest is to favour a particular type of technical standard, which is the harmonized standard (§ 6). We believe that with this choice the European Union is trying to convey what is already intuited by the definition of European cybersecurity-technical standardization to public ends by pursuing policy objectives.

71 Let it be permissible to refer to Serini 2023a.
72 Rybnicek, Plakolm and Baumgartner, 2020.

Problems arise, however, both on the definitional level, given the labile limit of the nature of these standards, which although technical are strongly close to legal, and on the level of rights protection guarantees. Although since the James Elliott Construction ruling in 2016, the Court of Justice has judged these standards to be an integral part of Union law and, most recently, with the Public.Resource.Org ruling in March 2024, the Court has recognized their free and full accessibility to the public, it is still doubtful whether rights that may be affected by these standards can be enforced through direct judicial action against a harmonized standard.

The issue appears to take on particular significance in the context of security, where the substance of the regulation defines the extent to which freedoms and rights can be constrained for security reasons.

Far from having exhausted such a complex topic, the hope is to have raised questions that may stimulate further studies and in-depth analyses on the subject, thereby fostering scientific debate on the matter.

References

Abrahamsen R., Leander A. 2016., *Handbook of private security studies*, London.

Aliquò G. 2023, "Sicurezza pubblica e sicurezze private", *Polizia moderna*.

Bombelli G. 2017, "Dal moderno all'ultramoderno'? Intorno al nesso diritto-tecnica-sicurezza", in Pizzolato F., Costa p. (a cura di), *Sicurezza e tecnologia*, Milano: Giuffrè.

Bombelli G. Farah p. , "The Interlinkages Science-Technology-Law: Information and Communication Society, Knowledge-Based Economy and the Rule of Law", *Legal Studies Research Series*, n. 43.

Bourdeau p. 2013, "Resiliencism: premises and promises in securitisation research", *Resilience: Inter-national Policies, Practices, and Discourses*, 1(1).

Broadbent J. and Laughlin R. 2005, "Public-private partnerships: An introduction", *Accounting, Auditing & Accountability Journal,* 18 (6): 744-755.

Buzzacchi C. 2015, "Sicurezza e securization tra Stato, Unione Europea e mercato: prerogative dei pubblici poteri o attività economica?", in Pizzolato F., Costa p. (a cura di), *Sicurezza, Stato e mercato*, Milano: Giuffrè.

Carr M. 2016, "Public–private partnerships in national cyber-security strategies", *International Affairs*, 92 (1): 43-62.

Castaldo F. 2018a, "Fronteggiare il nemico in arene competitive turbolente: l'importanza della fiducia e delle capacità dinamiche nelle alleanze strategiche", *Rivista Italiana di Conflittologia*, 35: 10-39.

Castaldo F. 2018b, "I sistemi di gestione del traffico aereo e l'incombente minaccia del crimine: la necessità di un modello cyber security centric", *Rivista Italiana di Conflittologia*, 36: 29-48.

Castaldo F. 2019, "Dalla Cyber Defense alla Cyber Resilience dell'Infrastruttura Critica. Alcune implicazioni strategiche e organizzative", *Rivista di Economia e Politica dei Trasporti*, 3: 1-10.

Castaldo F. 2021, *Resilience by Design and Resilience Embedded. Achieving Proactive Cyber Defense*, Benevento: CUAM University Press.

Castaldo F. 2023, "Traghettare le organizzazioni nell'era delle incertezze", *Sviluppo & Organizzazione*, 311:44-48.

Castaldo F. and Serini F. 2024, "La collaborazione pubblico-privata nell'ambito della Cybersecurity europea. Dal piano organizzativo a quello della normazione tecnica", *Intervento presentato al Convegno Internazionale Interdisciplinare su "Cybersecurity e Istituzioni Pubbliche. Rischi e opportunità della regolamentazione informatico-giuridica di un fenomeno trasversale*", Novara, 23 maggio 2024.

Castaldo F., Porretta p. , Zanda S. 2024, "Recovering the dormant values of accounting to navigate the challenges of the 2030 agenda and beyond", *Meditari Accountancy Research*, 32, 6.

Cerf V. 2022, "Sulla governance di Internet", in Abba L., Lazzaroni A., Pietrangelo M. (a cura di), "La Internet governance e le sfide della trasformazione digitale", in *Rivista Italiana di Informatica e Diritto*, fasc. 4.

Della Morte G. 2018, *Big Data e protezione internazionale dei diritti umani. Regole e conflitti*, Napoli, 2018.

Dunn Cavelty M. and Suter M. 2009, "Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection", *International Journal of Critical Infrastructure Protection*, 2 (4): 179-187.

Dunn Cavelty M., Eriksen C. and Scharte B. 2023, "Making cyber security more resilient: adding social considerations to technological fixes", in *Journal of Risk Research*, 26(7): 801-814.

Eckert S. 2005, "Protecting Critical infrastructure: The Role of the Private Sector", in p. Dombrowski (Eds) 2005, *Guns and Butter: The Political Economy of International Security*, Boulder: Lynne Rienner Publishers.

Elias G. 1995*,* "Le regole comunitarie per l'accesso al mercato unico: le misure per l'eliminazione delle barriere tecniche", in Andreini p. , Caia G., Elias G., Roversi-Monaco F.A. (a cura di), *La normativa tecnica industriale. Amministrazione e privati nella normativa tecnica e nella certificazione dei prodotti industiali*, Bologna, Il Mulino.

Eweje G., Sajjad A., Nath S.D. and Kobayashi K. 2021, "Multi-stakeholder partnerships: A catalyst to achieve sustainable development goals", *Marketing Intelligence & Planning*, 39 (2): 186-212.

Farrand B., Carrapico H. 2018, "Blurring public and private: cybersecurity in the age of regulatory capitalism", in Bures O., Carrapico H. (a cura di), *Security Privatization. How non-security-related Private Businesses Shape Security Governance*, Cham.

Gallotti C. 2022, *Sicurezza delle informazioni. Gestione del rischio. I sistemi di gestione per la sicurezza delle informazioni. La norma ISO/IEC 27001:2022. I controlli della ISO/IEC 27002:2022*, Lulu press.

George G., Fewer T.J., Lazzarini S., McGahan A.M. and Puranam p. 2024, "Partnering for grand challenges: A review of organizational design considerations in public-private collaborations", *Journal of Management*, 50 (1): 10-40.

Greco N. 1999, "Crisi del diritto, produzione normativa e democrazia degli interessi. Esemplarità della normazione tecnica in campo ambientale", in Aa.Vv., *Crisi del diritto, produzione normativa e demo-crazia degli interessi*, Edistudio, pp. 37 ss.

Grimsey D. and Lewis M. 2007, *Public private partnerships: The worldwide revolution in infrastructure provision and project finance*, Edward Elgar Publishing.

Hachez N., Wouters J. 2011, *A Glimpse at the Democratic Legitimacy of Private Standards: Assessing the Public Accountability of GlobalG.A.P.*, in *Journal of International Economic Law*, 14 (3).

Hemming R. 2006, *Public-private partnerships*, International Monetary Fund.

Heritier p. 2003, *Urbe-Internet. Vol. 1. La rete figurale del diritto*, Torino, Giappichelli.

Hodge G.A., Greve C. and Boardman A.E. (Eds) 2010, *International handbook on public-private partnership*, Edward Elgar Publishing.
Irti N. 2006, *Norma e luoghi*, Roma-Bari: Laterza.
Kamara I. 2017, "Co-regulation in EU personal data protection: the case of technical standards and the privacy by design standardisation 'mandate", *European Journal of Law and Technology*, Vol 8, n 1.
Kshetri N. 2015, "India's Cybersecurity Landscape: The Roles of the Private Sector and Public-Private Partnership", *IEEE Security & Privacy*, 13 (3): 16-23.
Kumar Muthusamy S. 2014, "Role of context and contest in the structuring of alliance governance", *Journal of Strategy and Management*, 7 (2): 172-192.
Laughlin C. 2015, "Cybersecurity in Critical infrastructure Sectors: A Proactive Approach to Ensure Inevitable Laws and Regulations Are Effective", *Journal on Telecommunication and High Technology Law*, 14: 345.
Lessig L. 1999, *Code and Other Laws of Cyberspace*, New York.
Lichtenthaler U. 2016, "Alliance portfolio capability: a conceptual framework for the role of exploration or exploitation alliances", *Journal of Strategy and Management*, 9 (3): 281-301.
Luiijf E., Besseling K. and De Graaf p. 2013, "Nineteen national cybersecurity strategies", *International Journal of Critical infrastructures* 6, 9 (1-2): 3-31.
Min K.S., Chai S.W. and Han M. 2015, "An international comparative study on cybersecurity strategy", *International Journal of Security and Its Applications*, 9 (2): 13-20.
Moore T. 2010, "The economics of cybersecurity: Principal and policy options", *International Journal of Critical infrastructure Protection*, 3 (3): 103-117.
Mosca C. 2012, *La sicurezza come diritto di libertà. Teoria generale delle politiche della sicurezza*, Padova: Cedam.
Mulyani S. 2021, "Critical success factors in public-private partnership", *Journal of Accounting Auditing and Business,* 4 (1): 81-86.
O'Mara M. 2019, *The Code: Silicon Valley and the Remaking of America*, New York.
Oddenino A. 2018, "Digital standardization cybersecurity issues and international trade law", *Questions of International Law*, n. 51.
Pellicelli A.C. 2012, "Strategic alliances", *Economia Aziendale Online*, 2: 1-21.
Pollicino O., Bassini M., De Gregorio G. 2022, *Internet law and protection of fundamental rights*, Milano: Bocconi University Press.
Pollicino O. 2023, *Potere digitale*, Estratto da I Tematici, V-2023, Potere e Costituzione, in *Enc. dir.:* 415.
Rogers J. 2016, *Public-private partnerships: A tool for enhancing cybersecurity* (Doctoral dissertation, Johns Hopkins University).
Rossa S. 2023, *Cybersicurezza e pubblica amministrazione*, Napoli, Editoriale scientifica.
Russel D., Gangemi G.T. 1991, *Computer security basics*, Sebastopol: O'Reilly Media.
Sarmento J.M. and Renneboog L. 2016, "Anatomy of public-private partnerships: their creation, financing and renegotiations", *International Journal of Managing Projects in Business*, 9 (1): 94-122.
Sassen S. 2008, *Territory, Authority, Rights: From Medieval to Global Assemblages*, Princeton.
Serini F. 2023a, "La frammentazione del cyberspazio merceologico tra certificazioni e standard di cybersicurezza. Alcune considerazioni alla luce delle discipline europea e italiana", *Rivista italiana di informatica e diritto*, 2.
Serini F. 2023b, "Il sistema europeo di cooperazione informativa per il contrasto alle minacce informatiche. Verso una definizione di cybersicurezza integrata?", *MediaLaws*, 3.
Serini F. 2024, "Collective cyber situational awareness in EU. A political project of difficult legal realisation?", *Computer Law & Security Review*, 55.

Suter M. 2012, "PPPs in Security Policy: Opportunities and limitations", *CSS Analyses in Security Policy*, 111.
Thomas R.N. 2013, *Securing Cyberspace Through Public-Private Partnership: A Comparative Analysis of Partnership Models*, Center for Strategic & International Security.
Ursi R. 2022, *La sicurezza pubblica*, Il Mulino, Bologna.
Vining A.R. and Boardman A.E. 2008, "Public-private partnerships: Eight rules for governments", *Public Works Management & Policy*, 13 (2): 149-161.
Volpato A. 2024, "Il ruolo delle norme armonizzate nell'attuazione del regolamento sull'intelligenza artificiale", *Associazione Italiana Studio di Diritto dell'Unione Europea*, 2.
Volpe A. and Castaldo F. 2021, "Complessità, incertezza e urgenza di agire", *Sviluppo & Organizzazione,* 297: 34-40.
Volpe A. and Castaldo F. 2024, "Rational choice and actors' strategic interdependence: an insight into game theory", *Il Pensiero Economico Moderno*, 1-2: 11-40.
Watkins B. 2014, "The impact of cyber attacks on the private sector", *Briefing Paper, Association for International Affair*, 12: 1-11.
Zanda S. and Castaldo F. 2023, September, "Epistemology of complexity in a state of crisis. Leadership and coordination as catalysts of neghentropy", *16th Annual Conference of the EuroMed Academy of Business*.