Crime Law Soc Change (2017) 67:265–288
DOI 10.1007/s10611-016-9653-3

A typology of cybersecurity and public-private partnerships in the context of the EU

Raphael Bossong[1] · **Ben Wagner**[2]

Published online: 14 October 2016

Introduction

Current discussions on security on the Internet mostly revolve around the necessity and limits of *public* action in the face of a decentralised and privately owned or operated space [1, 2]. Unsurprisingly, the question of public authority particularly comes to the fore in matters of security. The original vision of an entirely self-regulated as well as resilient, decentralised Internet has come under severe stress due to structural vulnerabilities beyond the reach of any individual actor [3]. These vulnerabilities are increasingly exploited by a growing number of harmful actors, which are also increasingly putting their services and malware products on sale and wide access. This calls for more multi-faced and coordinated governance approaches to improve security on the Internet that is typically termed 'cybersecurity' [4].[1] In short, to provide cybersecurity public and private actors clearly need to engage with each other [5]. This is reflected in a growing number of policy initiatives and public declarations that underline the value of Public Private Partnerships (PPP) for increasing or providing cybersecurity [6]. Such partnerships are also critical site to translate broad or ambiguous conception of cybersecurity, which may have reinforced the trend towards an ever more encompassing securitisation of contemporary Western societies, into daily practices.

However, the interaction or partnership between public and private actors for cybersecurity can take many institutional shapes and forms (see also Bures in this issue), which remain obscured by an overly encompassing and ambitious political rhetoric [7]. One can

[1] One should, however, that there are alternative framings of technical IT security and problems with the general label of "cyber", which will be briefly taken up below.

✉ Raphael Bossong
raphael.bossong@swp-org.de

Ben Wagner
bwagner@europa-uni.de

[1] German Institute for International and Security Affairs, Berlin, Germany

[2] Europe University Viadrina, Frankfurt, Germany

point to considerable gaps between public rhetoric and practice of security cooperation with private actors [8] - or see this cooperation as comprehensive "dataveillance" [9], whereby public actors access a hitherto unimaginable depth of information that consumers are structurally inclined to provide in exchange for free online services and software applications. For instance, the NSA scandal has revealed substantial evidence for public-private collaboration, whereas the current debate on the legitimacy of strong commercial encryption underlines that the relationship between "national security" and private authorities is at least as often fraught with tension and confrontation.

Even more broadly speaking, this relates to a fundamental conceptual and political debate on the evolving nature of security governance (see editorial by Bures and Carrapico), which has challenged conventional understandings of modern statehood and foundations of public authority [10, 11]. In particular, the provision of security has been traditionally understood as the first-and-foremost responsibility of the state, as the legitimate bearer of the monopoly on the use of legitimate violence, but increasingly involves a much wider array of actors, be they companies, private individuals, civil society organisations or international organisations. Networks of security governance can be considered a functional adaptation to increasingly networked and transnational risks and threats, such as terrorism or critical infrastructure failure, while also balancing some of the problematic tendencies of state security apparatus by including a wider range of voices and perspectives [12]. At the same time, security governance that moves away from public authorities generates multiples challenges and critical questions [13–15], be it with regard to the sheer number of actors at multiple levels (compare Biaumet and Aarstad in this issue) or the exercise of coercive powers for profit (compare Saldivar in this issue).

Against this complex background, this paper does not stake out a clear position for or against public-private cooperation for cybersecurity. It does not appear feasible or realistic to disentangle the level functional interdependence and geographical extension of security governance networks, especially in the area of information communication technologies (ICT). Rather, it pursues a more modest, but – in our view – nonetheless essential aim, namely to clarify our understanding and conceptualisation of the varied forms and kinds of PPPs in the area of cybersecurity, especially in so far as it concerns more regular and publicly known forms of cooperation.[2] It then applies this understanding to the case of the EU that arguably constitutes a representative, relatively transparent and significant case for such regular kinds of PPPs for cybersecurity.

These steps reflect in two parts of the paper. First, we argue that ideal-typical PPPs focus on operational provision or delivery of services - or policy implementation in a broad sense -, in contrast to other forms of policy consultation, shared regulation and interest representation. Furthermore, PPPs likely to benefit from formalised agreements that specifies intended benefits or profits as well as the risks of the venture. Yet we also note that the ICT sector exhibits some distinct characteristics, which may explain some of the confusion about the possible meaning of PPPs. In particular, "cyberspace" and the respective manifestations of "cybersecurity" play out at multiple levels and among varied communities of practice, ranging from infrastructural issues to the management of online content. A corresponding typology helps to map different actor incentives as well as normative concerns with regard to the range of possible public-private interactions for cybersecurity. However, such an abstract representation necessarily glosses

[2] In contrast to informal working arrangements for security and intelligence agencies

over many important nuances and still needs to be situated in particular empirical context.

With these considerations in mind, the second part of this article applies this heuristic framework to survey the EU's efforts to develop PPPs for cybersecurity [16, 17]. It has to be underlined that EU member states remain mainly responsible for the provision of "internal security", which can include cyberspace, following the example of technologically advanced North-Western European states, such as the UK, Germany or the Netherlands. One can also point to wide variety of platforms, alliances and initiatives for cybersecurity at European national as well as wider global levels,[3] so that the EU does not necessarily take a central position in wider transnational governance efforts for cybersecurity. Yet the EU is building a wide transnational regulatory regime on cybersecurity [18] and can exercise significant influence with regard to the large number of European states that have yet to formulate respective policies, processes and structures. In particular, the EU cybersecurity strategy extensively stresses the importance of public private interactions for cybercrime and cybersecurity [19], while the EU's recent agenda on internal security ([20], 20) argues that "cooperation with the private sector is also of critical importance, with public-private partnerships to structure a common effort to fight online crime."

Moving beyond these official declarations, the second part of this paper reviews the internal differentiation and diversity of EU PPPs for cybersecurity. The EU has doted itself with two agencies or centres that can participate in more regular administrative or operational aspects of cybersecurity, namely the European Network Information Security Agency (ENISA) and the EC3 cybercrime centre in EUROPOL. ENISA seeks partnerships for improving the technical reliability and resilience of cyberspace or critical information infrastructures, which are in private hands (compare Farrand and Carrapico in this issue). In contrast, the EC3 seeks out more operational exchanges with IT security companies in order to address cybercrime and complex threats, such as botnets, in a more proactive manner. In addition, the EC3 and its host institution EUROPOL seek to extend voluntary mechanisms for Internet content control with private actors, which has recently given rise to the so-called Internet Referral Unit. Related content control measures have given rise to a particularly critical discussion in its own right, but may also be usefully be thought of as a variant of wider patterns of PPPs for cybersecurity.

In conclusion, the proposed typology of public-private interactions helps to develop more systematic and analytical arguments about the development or relative stagnation of different kinds of PPPs for cybersecurity. It also underlines the need to focus normative critiques on specific cooperation dynamics, such as information sharing and active assistance, which need to be evaluated against wider legal and political principles that the EU officially endorses. Finally, the conclusions also return to the argument for more contractual or formalised PPPs, which should be evaluated in further research on the dynamically evolving relationships between public and private actors in the cyber realm.

[3] For instance, https://www.icspa.org/ or https://www.ncia.nato.int/NewsRoom/Pages/140918-NATO-launches-Industry-Cyber-Partnership.aspx

Towards a more structured conceptualisation of PPPs in cybersecurity

Public private partnerships in ICT

The rise of public private partnerships - as one component of the so-called New Public Management and more neoliberal models of the role of the state – initially grew out the privatisation of public infrastructure and as a means for attracting private resources for further public construction projects [21]. As the next logical step, PPPs spread to the management and general provision of public services that are based on these infrastructures, such as hospitals, schools or even prisons [22]. Over the last two decades this development has led to an extensive international debate on the merits and drawbacks of PPPs [23]. For instance, opinions diverge on how far economic efficiency should remain the main standard for assessing the merits of PPPs, or whether other values, such as fairness and equity in access to public services can also be enhanced or at least maintained in such contexts [24, 25]. Further critical questions are asked about the accountability of both public and private actors, and the transparency of their mutual agreements beyond formal administrative structures [26, 27]. Finally, one must also recognise that different state traditions, or political cultures, influence respective assessments [28]. Alongside efforts for standardisation by international organisations [29, 30], one continues to observe major cross-national differences in PPPs, including government support, dedicated institutions or agencies, laws, technical expertise [31] as well as more informal norms, historically grown economic structures and societal values [32].

This level of empirical diversity as well as debate about relative merits may explain why the term PPP is still often used without precision [33]. Nevertheless, mainstream PPPs are typically based on an explicit or formalised agreement, which tasks private actors with the provision of a public service, maintenance of infrastructure or new construction project. Such PPPs should also specify matching responsibilities, profit and risk sharing arrangements [34], which follows conventional economic reasoning on the need for calibrated (financial) incentives and control instruments to align the interests of self-interested rational actors [35]. However, standard commercial contracts cannot address all potential problems of PPPs, especially in high-risk projects or with regard to long-term partnerships agreements, so that there is a need for flexibility, learning and adaptability over time [36]. Some analysts emphasise further demanding and intangible standards for PPPs, whereby a shared sense of objectives, trust-based relations and synergetic use of the capacities of both public and private actors beyond cost considerations are the most central feature [37].

However, the main driver for the formation of typical PPPs are cost and efficiency considerations – or related policy beliefs – among public authorities. As summed up by Bovis [38]: “A common definition on public-private partnerships does not exist. However, ….[t]he method of financing and the risk transfer from public to the private sector are common features in different jurisdictions across the world...The principal benefit from involving the private sector in the delivery of public services through a public-private partnership format has been attributed to the fact that the public sector does not have to commit its own capital resources...and that substantial transfer of risks to the private sector offers value for money.”

Yet in the contemporary ICT sector the relations between public and private actors exhibit distinct features [39]. Unlike many other key economic and societal

infrastructures, the internet is a dominantly private construct, at least since its extremely dynamic spread and development since the early 1980s [40, 41]. This means that classic PPPs for construction and service provision are comparatively rare - at least in non-rural areas, advanced economies or with regard to standard infrastructures for telecommunications [42, 43]. Instead, PPPs serve as broad rhetorical instruments to influence private actors that operate, underpin and provide cyberspace, its logical interfaces and content, tying in with wider political discourses on innovation, competitiveness as well as national security [7]. This has given rise to the situation whereby an extremely wide range of policy initiatives, forums and consultation platforms in the ICT sector have been labelled as PPPs [44], which adds to, or surpasses, the existing definitional problems with conventional PPPs as outlined above.

In fact, when approaching the problem of security and safety in other infrastructure and industrial sectors one would expect classic debates on the need for binding regulations or liability rules versus considerations about economic competitiveness [45]. The wide range of voluntary and private governance instruments – which go under multiple labels, such as corporate social responsibility or, in the EU-context, the open of method of coordination – are frequently reviewed as a potential alternative to hierarchical regulation due to speed, flexibility, range and support from stakeholders in implementation processes [46, 47]. And as mentioned in the introduction, this corresponds to general arguments about the benefits of security governance that breaks out of the mould of the hierarchical security state. The classic counter-argument is to highlight the necessary "shadow of hierarchy" to make soft law effective [48, 49] - or to trace the evolution of soft law to increasingly hard regulation over time, as it becomes evident that not all private actors make the necessary "non-productive" investments into security [50].

Such familiar debates currently play out in the ICT sector, where the growing regulatory ambitions of public authorities competes with long-standing private approaches to self-governance [51]. Most recently, this can be illustrated by the European directive for Network Information Security [52], which emulates and advanced various related national provisions on mandatory security standards and reporting among relevant infrastructure providers and dependent operators (see Farrand and Carrapico in this issue).[4] However, the ICT sector continues to present particular challenges in terms of technical complexity, speed of change, diversity of participants and transnational interdependence, so that conventional policy-making remains constrained or needs to be complemented by alternative processes. Here one can refer the dynamically growing literature on "internet co-regulation" between public and private actors [53, 54] as well as the related notion of "multi-stakeholder governance" [55–57], which is as often conflictual as cooperative. Therefore, we cannot rule out, or delimit, the term PPP at this level of generality, but first need to disentangle the specific institutional relationship involved as well as the characteristics of cybersecurity that should be advanced to clarify the forms of cooperation in the context.

[4] At the time of writing, the legislative proposal had gained political agreement from all EU institutions, but was not formally concluded yet. See: https://ec.europa.eu/digital-single-market/en/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation

Public-private cooperation and governance tasks for cybersecurity

Just as the notion of PPPs, "cybersecurity" is characterised by a lack of specificity - especially when moving beyond technical understandings of information security that focus on the confidentiality, integrity and availability of computer system.[5] Arguably, the cyber label has opened a discursive door that provides an ever more expansive understanding of the shape and scope of the object to be secured, which may empower public security authorities [58, 59] and affect the wider conduct of international relations [60]. Precisely for this reason, it is useful to take a step back from high-level debates and to sketch out a more applied perspective on cybersecurity that takes multiple levels or dimensions of cyberspace into account.[6] These levels and dimensions are relevant to the analysis of PPPs as they are constituted by different actors or professional communities with different incentives for cybersecurity. For instance, a security engineer in a private company may rather consider himself part of a transnational community for a specific aspect of information security than responsible for national cybersecurity [61], which – in turn – shapes the possible range or format for respective partnerships.

To delineate the possible diversity of these communities, Choucri and Clark [62] provide a useful heuristic, which extends technical notions of IT network and internet architecture to broader social and information dimensions. Thus, cyberspace is constituted by, and cybersecurity plays out at,

1. the physical infrastructures layer (cables, IXP, etc.)
2. the layer of logical interfaces that are used to run and connect these infrastructures
3. the layer of content/information flowing across or being stored on these networks and
4. the layer of users (individual as well as corporate) that operate or depend on these systems.

The first two technical layers are critical to systemic cybersecurity, but are not necessarily reliant on public intervention [63]. Due to economic interests in business continuity, private companies that own, provide, manage or operate infrastructures for cyberspace can be expected to make considerable investments in network reliability and resilience. At the same time, information security experts and engineers have long developed close networks for cooperating on technical issues that underpin the global internet infrastructure on a global scale [64]. This explains why the respective efforts of states and international organisations to regulate the infrastructural dimension of the internet [65] continues competes with strong self-governance mechanisms by these

[5] Information and computer scientist tend to prefer other more technical and precise concepts, such as information security, which is composed of definable attributes of integrity, availability and confidentiality. Security scholars, in contrast, have highlighted the dangers of "securitizing" the digital communications or simply just 'cyber' and merging distinct issues of cybercrime, cyber-assisted crime with more state-centred notion of security, which can legitimate "offensive" methods and the involvement of the military.

[6] Again, we cannot go into the question whether cyberspace is a suitably precise analytical concept. For a widely cited official definition, see http://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf

private actors[7] – at least in liberal states that publicly refrained from direct control, while Western companies take on a matching central role [66].

The situation is at least as complex with regard to the second layer of applications. Private and largely confidential expert networks have long exchanged information on vulnerabilities and coding errors, not least as there is also a considerable reputational issue towards customers. Users are thus being provided with free software updates and vulnerability patches on a regular basis, even if the frequency with which this happens – and the growing commodification of vulnerabilities - also fuels a critical discourse on structural weaknesses and vulnerabilities of the commercial software market [67, 68].[8] The most fundamental approach to full self-regulation in this area is the open source movement that aims to provide better and more secure software on the basis of voluntary, transparent and largely non-remunerated collaboration of programmers around the globe. Conversely, there are also growing public efforts for certification and regulation that establish product liability and security standards for software providers [69, 70]. In a nutshell, the early catch-phrase that "code is law", which can be interpreted to mean that software code directly constitutes its own binding set of rules and behavioural constraints, is being complimented by complex legal frameworks for product regulation, especially when it comes to increasingly autonomous and interdependent software-based systems.

When moving to the content and user layer, Internet Service and especially Content Providers and Social Media Companies and other public-private interaction dynamics move centre-stage [71]. A standard assumption is that these actors do not have a direct commercial interest in public definitions of "security" beyond their service continuity and expanding the range of users [72, 73]. This can, but does not have to, imply protecting their platforms and services from malicious actors, as far as these threaten to highjack bandwidth or related technical service capacities, as in the case of botnets and spam [74]. However, it is economically costly and technologically challenging to implement more rigorous controls on exchanged content, while a conventional understanding of the internet would emphasise its "end-to-end" nature, i.e. the primary responsibilities of senders and receivers rather than intermediaries of information, and the corresponding "neutrality" or equality of data packages that flow across network [75]. Furthermore, monitoring problematic (non-verbal) internet content cannot be fully automated at this stage, and therefore tends to require comparatively costly human resources for reviewing flagged items. At the same time, it is clear that liberal political systems require some degree of cooperation from these providers to maintain legal norms about the limits of expression and the respect for human dignity [76].[9] This has led to complex trade-offs and variants between legal and voluntary governance arrangements for content control [49, 77, 78], which briefly returned to in the second part of this paper.

Finally, the fourth layer of users encompasses actor-centred, rather than technical or data-driven, dynamics in cyberspace. This is necessarily a very broad residual category

[7] For instance, http://www.ix-f.net/ixp-models.html. See also Farrand and Carrapico in this issue for a more detailed discussion on the historical development from public to private management of critical infrastructures.
[8] An especially controversial response to this challenge has been to create separate market incentives through programs such as 'bug bounties.'
[9] Such as "hate" speech, weapons instructions, child sexual abuse material, etc.

where one cannot clearly separate security-conscientious actors from the supposedly rather passive and security-insensitive mass of (corporate or individual) users [79, 80].

Building on this layering and heuristic parsing of communities for cybersecurity, we propose a cross-cutting differentiation between five broad areas or tasks of public private interactions for cybersecurity. According to a descriptive functionalist logic[10] these tasks are: 1) the reliable *provision* of internet/ICT access; 2) the co-*regulation* of technical security as well as of data handling; 3) the *exchange of information* on threats and vulnerability; and 4) *mutual assistance* in addressing known threats or illegal content in cyberspace. These tasks can be related to the previous critical discussion on the possible meaning of PPPs. In particular, these tasks need to be applied across various considerations of cybersecurity until here.

Concerning provision of service, it has already been mentioned that access to ICT infrastructures and the internet (in the West) has largely been provided by the private sector without formal requests from public actors, which limits the classic uses of PPPs for construction. As also referred to above, market regulation, that deals with possible externalities of economic activities, such as pollution, risks of accidents, eroding social security, etc., can involve various forms of hard law and soft governance. This could be likened to coordination in PPPs, but should - in our view – better be categories as other forms of soft governance, such as co-regulation or corporate social responsibility. In any case, in the area of ICT the initial bottom-up and non-governmental patterns of self-regulations that characterised the early days of the internet are increasingly replaced or complemented by national and international legal instruments,[11] which will also be illustrated in the second part of the paper.

The third task of information exchange between public and private actors, in contrast, is closer to the notion of an implementation or service-oriented partnership. Both public and private organisations should profit from up-to-date assessment of specific cyber threats and vulnerabilities, while strategic data aggregation should help to address more structural problems of under-investments in IT security. Such threat awareness should alert potential targets of the substantial level of risk, even if they lack specific experience with cyberattacks and consider themselves an unlikely target [81–83]. Systems and processes for information sharing between public and private actors should also cut down on response times to cyber incidents, which is especially significant when moving beyond data-losses or -thefts towards potential outages of major services (e.g. banking) and infrastructures (e.g. energy).

Nevertheless, public-private information sharing on cyber threats and incidents is beset by various cooperation problems and challenging externalities [84, 85]. Among other issues, it is mistaken to assume a general positive impact for all participants of information-sharing exercises. Many actors apparently fear the reputational costs of, or

[10] These functionally differentiated tasks or processes have been inductively derived by the authors from the diverse social science literature on cybersecurity referred above. For reasons of space this differentiation cannot be systematically related to wider theories of public (economic) regulation and security governance here, but this may prove a worthwhile research agenda for the future. On the one hand, one could test whether the proposed tasks are truly exhaustive and comprehensive in the area of cybersecurity. On the other hand, more elaborate formal reasoning on collective action dynamics, such as with regard to the public good qualities of information or reliable access, could be explored beyond the cursory remarks made below.

[11] If one applies a broad or multi-level understanding of cybersecurity, this can range from questions of rights management, privacy and data protection to secure communication protocol standards or product safety and security.

possible liabilities deriving from, breaches of their cybersecurity more than desiring the rather diffuse benefits of strategic threat awareness [86]. This explains the trend away from partnership towards mandatory public regulation and regulated institutional processes for a "duty to notify" in cases of major ICT incidents [87].

Alternatively, the general risks of cyberattacks may not dominate over the specific and costs for up-to-date mechanisms of protection. This can lead to collective problems [88], such as free-riding behaviour where individual actors may see themselves as too small to affect the wider level of IT security, so that they hope that other public players or dedicated IT companies will address the most serious threats. In any case, public and private actors are obviously extremely diverse, including global corporations, small and medium enterprises, local governments, non-technical line ministries or dedicated cyber units in defence ministries, just to name a few examples. As such, these actors have very different levels of human resources and technical capacities for engaging in cybersecurity (e.g.[89]). This explains why PPPs for information exchanges on cybersecurity mostly remain limited to comparatively exclusive clubs between major companies, be they infrastructure providers or global IT players, and dedicated cybersecurity authorities. In the US, this most clearly reflects in formalised and sector-specific centres for cyber-information sharing.[12]

The fourth area of active collaboration in addressing cyber-threats concerns an even smaller range of actors, but constitutes the most significant area for operational partnerships. Specialised IT security companies have an active commercial interest to buttress their visibility in the field, or may directly be tasked by public authorities for the provision of cybersecurity. This will be illustrated further below with regard to the EU cybercrime centre EC3, and may be conceptually related to the wider debate on privatised security governance and policing [13]. Yet other corporate actors beyond IT security firms may have a specific interest in operational cooperation with public authorities. For example, financial services experience particular exposure to cyberattacks and virtual thefts and therefore have a direct stake in respective criminal investigations [90]. Internet providers and social media companies provide another sector, where reputational costs of hosting extremist content has increasingly led them to partner with public authorities for monitoring and take-downs.[13]

Yet such proactive forms of assistance can create several normative problems. On the one hand, it is not clear in how far private actors have been drawn into 'pragmatic' cooperation that falls short of legal certainty and accountability for citizens, customers and users. For instance, it may be easier for private providers to block reported content than to develop a balanced assessment merit of each such request according to a different national and international legal standards [91]. On the other hand, public actors may be unduly empowered by drawing on private capacities to collect information that may then be used in criminal prosecutions or other executive actions [86].

A heuristic typology of PPPs for cybersecurity

To summarise these various considerations, we propose to a heuristic typology on public-private interactions in cybersecurity. It has been argued, albeit briefly that PPPs

[12] http://www.nationalisacs.org/#!member-isacs/jnog6

[13] http://www.wired.com/2015/11/facebook-and-twitter-face-tough-choices-as-isis-exploits-social-media/

in cybersecurity centre on information-sharing and active assistance, whereas basic service provision mostly remains in private hands.[14] At the same time, processes of internet co-regulation already constitute a highly complex issue are and should, at least for analytical purposes, be kept apart from the notion of PPPs. Furthermore, different layers of cyberspace reflect in different communities and incentives or disincentives for public-private cooperation across these tasks. While infrastructural and technical levels should not be excluded by definition, they tend to gravitate to the task of co-regulation with public actors, as general rule-setting is most significant for structural cybersecurity (Table 1).

As can be read from the following table, it is, therefore, the layers of content and users, and the functions of information-sharing and active assistance, that constitute the core of operational PPPs for cybersecurity. The table also indicates that other interactions as well as partnerships are possible. For instance, the NSA scandal highlighted that active assistance and access provided by infrastructural providers has been a key instrument for extensive intelligence collection. However, for reasons of space we cannot discuss every possible typological field, while it is also one of the core aims of the paper to provide more focus to the discussion on PPPs in cybersecurity. For these reasons, we consider it justifiable to limit the following discussion and empirical illustration to the identified "core" fields of PPPs for cybersecurity. But different reading and critique of the heuristic framework for focussing the link between PPPs and cybersecurity are certainly possible and deserve further attention.

Surveying EU cybersecurity and public private partnerships

The two EU agencies ENISA and EUROPOL are the main public operational or executive actors in the area of EU cybersecurity. Both actors are heavily dependent on cooperation with private actors for their organisational success, and are supposed to cooperate increasingly with each other. At the same time, they clearly have different mandates and respective relationships with private actors. The following overview therefore uses the typological differentiation with regard to the central tasks of PPPs, namely information-sharing and active assistance, and sets in relation to the different audience or layers that the two agencies appeal to.[15] By providing a structured overview of the types of relationships these organisations engage in, we hope to provide a clearer picture of what cybersecurity partnerships in this area actually look like in practice.

ENISA

ENISA, the European Union Agency for Network and Information Security, is the main organisation for structural cybersecurity, i.e. at the infrastructural and technical/logical level. ENISA was founded in 2004 and has gradually established itself as a leading provider of technical advice in Europe (see Farrand and Carrapico in this issue).

[14] This point can be unlined by the fact that PPPs for a more secure internet provision at the infrastructural level have not yet been funded in Europe, as illustrated by the failed idea of a "Schengen-net" for secure data transfers in Europe.

[15] The typological fields are referred to in the respective subheadings of the different sections

Table 1 The layers of content and users, and the functions of information-sharing and active assistance constitute the core of operational PPPs for cybersecurity

Function Layer (communities)	Provision	Co-regulation	Information-sharing	Active assistance
Physical Infrastructure (Private owners)	PPPs for physical installation and service provision	Rules for internet exchange points and cable operators	exchanges on mainly physical vulnerabilities	Allowing access to ICT infrastructures by security services
Logical Interface (IT expert community and software providers)	Publicly supported research for privately provided security standards	Technical standard-setting for network communication protocols and reliability of applications	Regular exchanges on code errors, exploits and vulnerabilities	Public-private cooperation to address vulnerabilities and incidents (CERT)
Content/data (Internet service providers, social media)	Voluntary hosting of public messages/ propaganda/ counter-narratives by private service providers	Multiple regulatory issues on content management, data protection, privacy protection, "regulated" access for security services, etc.	Reporting of problematic content to public authorities (e.g. radical websites)	Active filtering and take-down of content beyond formal regulatory requirements
Other actors that use or proactively defend ICT systems	Commercial provision of cybersecurity products and systems to public authorities	Definition of users with higher security and reporting requirements (e.g. other ICT-supported infrastructures)	Reporting on attacks and malignant actors, strategic threat awareness	Active collaboration in takedowns and prosecution of malignant actors

In particular, the agency produces a large volume of conceptual papers and organises exercises,[16] workshops and expert meetings on cybersecurity. In 2013, ENISA was given an expanded and permanent legal basis, which defined its organisational mandate as follows ([92], 43): "The Agency should contribute to a high level of network and information security, to better protection of privacy and personal data, and to the development and promotion of a culture of network and information security for the benefit of citizens, consumers, businesses and public sector organisations in the Union, thus contributing to the proper functioning of the internal market."

In light of this, regular interactions across the public-private divide are clearly essential to the work of ENSIA. At a very general level, this can be illustrated by the inclusion of private representatives in the so-called permanent stakeholder group, which should assist the management of ENISA after the last revision of its mandate.[17] But already well before, ENISA conducted extensive research on different models and potential of PPPs in the ICT sector [93], which supports several arguments made in

[16] ENISA has organised several annual major ICT incident exercises for EU member states that were triggered official EU conclusions in the aftermath of the 2009 Estonian cyber-attacks. Assessments of these exercises are limited to official document, where the large number of participants (500+) and positive resonance had highlighted

[17] See https://www.enisa.europa.eu/about-enisa/structure-organization/psg

the first part of this article. Thus, the agency underlines that private actors are often unwilling to share information on a voluntary basis and that formal agreements or structures are necessary to ensure the operational usefulness of PPPs to both private and public actors.

At the same time, the focus of ENISA on more infrastructural layers of cybersecurity suggests that public-private interactions are more likely to take the form of co-regulation for general standard setting or security certification.[18] This reflects in a range of multi-stakeholder governance forums overseen by ENISA, such as the "ENISA Internet infrastructure security and resilience reference group",[19] and the „Electronic Communications Reference Group (ECRG)"[20] These groups interact with other forums for technical self-regulation, mainly the International Standards Organisation (ISO), the European Electronic Standards Institute (ETSI, with MoU) and CEN CELENEC for further industrial standards.[21]

ENISA also engages in a range of wider educational and awareness raising activities that should stimulate greater cybersecurity investments among both public and private actors. Aside from a so-called awareness raising community of ENISA – which seems to have been discontinued after 2010 -,[22] the largest coordinated effort is the so-called cybersecurity awareness month, which includes various private organisations.[23] However, these educations activities cannot be considered as sustained and substantial PPPs, since its target audience is diffuse and participants are not expected to enter into more regular relationships with ENISA.

PPPs for information sharing (logical and user layer)

For more substantial PPPs for cybersecurity, one can instead turn to private forums for sector-specific information sharing and which have contacts to ENISA. Examples are the so-called European Financial Institutes – Information Sharing and Analysis Centre[24] (EU-FISAC), or the so-called European Cyber Security Protection Alliance (CYSPA),[25] which united both business and research institutions. A somewhat confusing array of additional private initiatives and platforms, such as the Internet Security Alliance for Europe and the Security Alliance for Europe, also interact with ENISA and comment on EU policy.[26]

However, the main PPP officially led by ENISA has been the so-called "European Public + Private Partnership for Resilience" (or *E3PR*). This initiative emerged in the context of a larger EU policy programme to increase the security of Critical Information Information infrastructures (CIIP) [94]. The E3PR format generated a number of

[18] See also Art. 3 of the EU regulation establishing ENISA (revised 526/2013)
[19] https://resilience.enisa.europa.eu/internet-infrastructure-security-and-resilience-reference-group
[20] https://resilience.enisa.europa.eu/ecrg
[21] https://www.enisa.europa.eu/publications/articles/standards-for-cyber-security
[22] https://www.cscan.org/openaccess/?id=213
[23] http://www.enisa.europa.eu/activities/stakeholder-relations/nis-brokerage-1/european-cyber-security-month-advocacy-campaign
[24] https://www.enisa.europa.eu/activities/cert/support/information-sharing/european-fi-isac-a-public-private-partnership. This has been modelled on a corresponding US Forum with global reach. http://www.fsisac.com/
[25] http://www.cyspa.eu/default.aspx?page=home
[26] http://www.scmagazineuk.com/internet-security-alliance-to-launch-european-spinoff/article/382265/ https://ec.europa.eu/futurium/en/system/files/ged/safe_-_nis_and_the_dsm_07042015.pdf

thematic working and expert groups that should exchange information on relevant vulnerabilities and define policy options (compare Farrand and Carrapico in this issue).[27] However, the E3PR failed to generate tangible results due to the diversity of stakeholders and avenues for action that could be considered before the EU proposed a more specific legislative agenda [95]. Information sharing channels for CIIP issues remained highly fragmented in Europe,[28] particularly when aiming to address the cross-sectoral vulnerabilities of infrastructures. A later official evaluation report of the E3PR underlined that that multiple conflicts of interests with regard to the confidentiality of data or prospect of costly mandatory security measures further hampered the emergence of the desired partnership [96].

By 2013, the EU already debated the aforementioned NIS directive [52], which should extend mandatory information sharing on cybersecurity incidents from telecommunications providers[29] to other critical infrastructure providers. Even before the directive has been politically agreed on in December 2015, ENISA created the so-called NIS platform to succeed the E3PR. By mid-2015, the NIS platform listed more than 200 members - with approx. 110 of them representing business interests -,[30] and had met at least five times. This indicates a substantial effort of public-private networking.

Yet the terminological change from a *partnership* to a *platform* for private industry is telling. Rather than promoting regular operational or administrative cooperation, as we would expect in a classic PPP, the NIS Platform has worked on a clearer agenda for co-regulation and related policy options. For these purposes, ENISA created three working groups, namely on risk management, information exchange and incident coordination and, finally, secure ICT research and innovation. Clearly, these tasks may also apply to operational PPPs, but at the time of writing, the NIS platform has not reached beyond several conceptual papers that were intended to prepare the implementation of the upcoming NIS directive.[31] This stakeholder consultation should also be viewed in wider international processes, as reflected in a recent and first EU US meeting in that format.[32] In sum, the NIS platform should mainly be regarded as a supporting process of regulatory governance of critical infrastructures.

[27] ENISA, 2012a. European Public + Private Partnership for Resilience. Activity Report 2012. Available at: https://resilience.enisa.europa.eu/ep3r/2012-activity-report.

[28] Compare also for an incomplete survey of information-sharing platforms across EU member states https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg2-documents/wg2-outcome-draft/at_download/file.

[29] This would hitherto be limited to some cases that are covered by the 2009 EU telecommunications regulation (Directive 2009/140/EC). See https://resilience.enisa.europa.eu/article-13

[30] Public authorities from 18 member state are taking part, while the rest is constituted by academic institutions or experts See full list of members http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=2920&NewSearch=1&NewSearch=1

[31] See https://resilience.enisa.europa.eu/nis-platform. Especially the second working group provide the most detailed recommendations on how to differentiate, improve and link up the variety of information-sharing initiatives for CIIP, see https://resilience.enisa.europa.eu/nis-platform/shared-documents/5th-plenary-meeting/chapter-3-wg2_final-for-discussion-may-27-2015/at_download/file

[32] https://resilience.enisa.europa.eu/nis-platform/shared-documents/eu-us-preliminary-workshop-comparing-approaches

Active assistance (logical and user layer)

Yet one point to another area where ENISA may take on a more operational role for cybersecurity with private actors already, namely via its support for Computer Emergency Response Teams (CERTs). CERTs[33] have been developed since 2006 onwards. At the time, a few member states had started to create such units in emulation of the US, which pioneered this instrument already in 1990s [97]. By 2012, a separate EU CERT has been created,[34] while regular network activities and standardization of procedures to coordinate the work of national CERTs were underway.[35] The web presence of the EU CERT further includes regular news items on cyber threats and vulnerabilities of various applications.

These CERTs arguably constitute of boundary case for PPPs as defined for the purposes of this paper. The leading US model is mainly public organisation, which maintains close contacts with private business.[36] Various national CERTs in Europe clearly have strong ties with the private sector[37] – or conversely, CERTs of leading IT providers, such as the German Telecom, maintain close contacts with the public sector, including the EU level.[38] The EU CERT Mechanism similarly lists various private companies and internet providers as "partners"[39] for regular information sharing. However, public authorities also increasingly seek to provide their own cyber response capacities without having to partner with, or to rely on, private assistance.[40] For instance, the so-called European Governmental Cert Group[41] and officially listed partners of the EU-CERT are purely made up of public authorities,[42] while a recent analytical paper uses the added qualifier of national CSIRTs (nCSIRTs), even if there remain significant interfaces with private actors [97]. So formalised governance networks can only be made out among public sector CERTs. This interpretation of CERTs as moving away from PPP should be tested in further comparative empirical research.

In sum, ENISA expresses strong support for public private partnerships for cybersecurity, but mainly acts as a facilitator for technical co-regulation and certification with private actors (at the logical and infrastructure layer). ENISA organises stakeholder consultations in relevant EU regulation on cyber and critical infrastructure, as in the NIS Platform, and supports general awareness raising on cybersecurity among both public and private actors. Yet there is limited evidence for more operational PPPs, as

[33] Or computer security incident response teams in alternative European parlance (CSIRT), see https://www.enisa.europa.eu/activities/cert/support/guide2/introduction/what-is-csirt

[34] http://cert.europa.eu/cert/plainedition/en/cert_about.html.

[35] For instance, one could point to frameworks for data sharing or best practice collection, see http://www.enisa.europa.eu/activities/cert/support/data-sharing
http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/the-directive-on-attacks-against-information-systems

[36] https://www.us-cert.gov/about-us

[37] http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

[38] https://www.telekom.com/verantwortung/sicherheit/136918

[39] https://www.enisa.europa.eu/activities/risk-management/events/enisa-workshop-on-eu-threat-landscape/05PresentationStavrosLingris p-15

[40] https://www.enisa.europa.eu/activities/cert/support/information-sharing/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs

[41] http://www.egc-group.org/index.html

[42] https://cert.europa.eu/cert//plainedition/en/cert_partners.html

official CERTs increasingly focus on the specific internal or defensive needs of public actors.

The EC3 and its public private partnership activities

In contrast, operational PPPs for serious cybercrime seem to be the quickly growing domain of the EC3. As the EC3 has only been created in 2013, it does not surprise that there is no academic literature on it yet. To date, one can only refer to a preparatory feasibility study by the RAND consultancy [98] that highlighted the challenges, but also the need for more coherent approach across European states in the fight against cybercrime. The EC3 was also created in a climate of austerity and thus with a tightly delimited budget, allegedly cutting into the human resource base of EUROPOL. Nevertheless, the EC3 quickly emerged as a significant actor in various international operations against botnets and serious cybercrime.[43] This is underpins, and is reinforced by, its intensive efforts to engage and partner with private actors.

Information sharing (users)

The EC3 has been flanked from the outset with two advisory groups, which included private corporate actors. One group is constituted by representative from security specialists, whereas the other gives a platform to the specific concerns of the financial sector. According to the initial terms of reference for the security-focused group,[44] the advisory group should, among other tasks, influence the strategic priorities of the new centre, inform various standards and define possible pilot projects for cooperation between the Centre and private IT security companies. This kind of private-public sector collaboration is not unusual in the IT security community and constitutes a relatively common form of cross-sectoral engagement beyond institutional boundaries [99]. Notably creation of these advisory groups does seem to be bearing fruit and there is evidence of regular and intense cooperation between the EC3 and financial service providers. A recent example is the cooperation of all major credit card providers in an EC3 led global operation against fraudulent air tickets sales.[45]

Building on its advisory groups, the EC3 has signed numerous Memoranda of Understanding (MoU) with private actors in the two sectors. To date at least four MoUs have been signed with financial actors or organisations,[46] adding to a larger number of agreements with IT security companies, such as Kaspersky,[47] McAfee,[48] Mnemonic,[49] Microsoft (security

[43] http://www.nttdata.com/global/en/insights/it-briefings/2015022401.html
[44] https://www.europol.europa.eu/sites/default/files/publications/ec3_programme_board_-_tor_-_terms_of_reference_and_mandate_of_the_advisory_group_on_internet_security.pdf
[45] http://www.computerweekly.com/news/2240235526/Over-a-hundred-cyber-criminals-arrested-in-global-operation
[46] Barclays, ING Group, Citibank, the European Banking Federation, and the association for ATM Security (EAST). See https://www.europol.europa.eu/category/news-category/agreements?page=1 and https://www.european-atm-security.eu/tag/ec3/ and http://www.finextra.com/news/fullstory.aspx?newsitemid=27536
[47] http://www.kaspersky.com/about/news/business/2014/Kaspersky-Lab-Broadens-Cooperation-with-Both-INTERPOL-and-Europol
[48] http://news.softpedia.com/news/Intel-and-Europol-Sign-Agreement-on-Fight-against-Cybercrime-465520.shtml
[49] http://www.eurosecglobal.de/europols-european-cybercrime-centre-ec3-and-mnemonic-co-operate.html

branch),[50] FireEye,,[51] Group IB,[52] AnubisNetworks,[53] and the Shadowserver Foundation.[54] The practice of such MoUs seems to reflect a wider trend in international cooperation, as evidenced by comparable agreements of INTERPOL with Kaspersky.[55] Microsoft, for its part, embedded the signing of MoUs with a global effort and networking, including the US and Latin America[56] and invested in a corporate cybercrime centre.[57] While the MoUs of the EC3 are not public, they seem to follow a common template that covers the exchange of "strategic" threat information, wider statistical information on security trends and of professional expertise. As far as can be inferred from public news items, the MoUs are limited to "non-operational" information.[58] These exchanges should help private actors to enhance their preparedness, while keeping the EC3 up-to-date on the latest security threats.

Active assistance (users)

The increasing formalisation of cooperation, such as in the form of a MoU, could be expected in light of the general characteristics of PPPs discussed above, which pointed to the use of explicit profit and risk-sharing arrangements. From an empirical perspective, this development could be related to current consultations by the European Commission on the value of further contractual arrangements for PPPs in the area of research for cybersecurity [100]. But this does not mean that the nascent EU arrangements for more operational assistance and partnerships in addressing cyber threats are already well specified or mature. In particular, the distinction between general information exchange, which the MoU are supposed cover, and further operational cooperation is maintained in practice. There is increasing number of publicised cases of direct cooperation of the mentioned IT companies with various European public authorities in criminal investigations, takedowns of botnets[59] and eliminations of Trojans.[60] It is

[50] http://iq-media.com/category/cybercrime/

[51] http://www.thepaypers.com/digital-identity-security-online-fraud/europol-s-ec3-joins-forces-with-fireeye-to-better-detect-cybercrime/761040-26

[52] https://www.europol.europa.eu/latest_news/europol-signs-agreement-group-ib-cooperate-fighting-cybercrime

[53] https://www.europol.europa.eu/newsletter/ec3-and-anubisnetworks-initiate-cooperation-fighting-malware-threats

http://www.so-co-it.com/post/368648/anubisnetworks-and-europol-s-european-cybercrime-centre-sign-memorandum-of-understanding-to-fight-international-malware-threats.html/

[54] https://www.europol.europa.eu/latest_news/shadowserver-foundation-steps-cooperation-europol-combat-cybercrime

[55] http://www.kaspersky.com/about/news/business/2014/Kaspersky-Lab-Broadens-Cooperation-with-Both-INTERPOL-and-Europol

http://www.informationsecuritybuzz.com/kaspersky-lab-broadens-cooperation-interpol-europol/

See on the joint EUROPOL INTERPOL MoU http://www.threatmetrix.com/interpol-has-new-nerve-centerand-more-muscle/

And conference http://www.interpol.int/News-and-media/Events/2014/INTERPOL-Europol-Cybercrime-Conference-2014/INTERPOL-Europol-Cybercrime-Conference-2014

[56] http://iq-media.com/category/cybercrime/

[57] http://news.microsoft.com/presskits/dcu/

[58] https://www.european-atm-security.eu/tag/ec3/

https://www.european-atm-security.eu/tag/ec3/

[59] http://blogs.microsoft.com/on-the-issues/2015/02/25/europol-takes-down-servers-used-by-cybercriminals-to-steal-financial-data/

[60] http://www.2uzhan.com/police-security-firms-team-up-and-take-down-shylock-malware/ This particular action even seems to have involved the British signals intelligence service GCHQ

conceivable that general threat and vulnerability information provided by private actor sufficed for a technical shutdown, but it is equally more than probable that personal information of owners of IP addresses or computers would have been uncovered in the process.

This ties in with the formation of the so-called J-CAT task force, which unites the EC3, seven European national partners,[61] the US, Canada, Australia and Colombia. The task force founded in autumn 2014 as a pilot project for transnational cybercrime investigations.[62] Although it is official constituted by public actors, participants also highlight the contribution of IT security companies, such as Anubis, Symantec and Microsoft, during operations [99]. The initial successes of the task force have created a momentum to put this flexible forum on a permanent basis.[63] Yet to date, there has been no clarification on the legal framework and respective powers of the task force and its associated private actors. Participants suggest that national legal frameworks and the use of 'lead states' for specific investigations provide a pragmatic solution (ibid, 145). This clearly reflects the perspective of security authorities that are interested in cross-national prosecutions, but needs to be critically evaluated by other judicial or civil society actors. Data protection issues or decisions on the appropriate legal basis for persecuting individual actors remain to be addressed based on transparent and consistent rules, rather than by ad hoc decisions which state, legal framework or cooperation arrangement with private actors could be brought to bear in a given instance.

Information sharing & active assistance (content)

The final and perhaps most controversial development of public-private cooperation and partnership for cybersecurity equally falls between the cracks of information-exchanges and active assistance on internet content. In 2015 EC3 has been flanked by the so-called "internet referral unit" (EU IRU) at Europol, in order to "combine the expertise of both EC3 and Europol's counter terrorism unit … to support the Member States in their endeavour to tackle online terrorism propaganda" ([101], 4). The unit should identify extremist online content, coordinate with national authorities on the respective recommended course of action (monitor or takedown), and make corresponding suggestions to private internet service providers and social media companies. The first months of operation of the new unit appear to have been comparatively successful, with a reported cooperation rate of 88 % of private industry with regard to flagged problematic content.[64] Officially, the EU maintains that the decision to take down content remains with the respective private company that hosts the content.[65] Yet

[61] Austria, France, Germany, Italy, Spain, the Netherlands and the UK

[62] http://sgocnet.org/site/wp-content/uploads/2014/06/08_ReitanoEtAl_pp142-154.pdf
http://www.theguardian.com/technology/2014/sep/01/europol-taskforce-cybercrime-hacking-malware
https://www.europol.europa.eu/content/expert-international-cybercrime-taskforce-launched-tackle-online-crime
http://www.scmagazineuk.com/europol-plans-more-malware-takedowns/article/396089/
https://www.clearswift.com/blog/2014/07/25/why-joint-cybercrime-action-taskforce-positive-europe
http://www.computing.co.uk/ctg/news/2348940/europol-cybercrime-head-international-public-private-collaboration-the-one-true-way-to-stop-cyber-criminals

[63] http://www.scmagazineuk.com/j-cat-operations-to-continue/article/422464/

[64] EU DOC 6785/16, p. 35

[65] http://www.adjacentgovernment.co.uk/ict/european-union-internet-referral-unit-europol/23582/

the high rate of compliance, as well as the related national experience of similar units, most notably the UK Counterterrorism Internet Referral Unit - which served as the organisational model for the IRU - suggest that the respective partnership with private industry is increasingly structured.[66] For instance, UK authorities have been awarded so-called "super-flagger" status by platforms such as Youtube, which exemplifies the regularisation of this kind of cooperation.[67]

The IRU is already connected to the wider "EU-level Forum with IT companies", which since late 2015 unites major players, such as Google, Facebook, Microsoft and Twitter to improve their cooperation with content control measures, but has been criticized by NGOs for a lack of transparency and wider participation.[68] These initiatives also build on the previous European efforts, the so-called "Check-the-Web" portal hosted at Europol since 2008 and the 2010 'CleanIT' project that sought to build links between the private sector and public sector and to draft shared 'best practices' in addressing 'terrorist use of the internet'.[69] This led to the so-called European Joint Initiative on Internet Counter Terrorism (EJI-ICT) to develop another network of national contact points for content monitoring. However, already the CleanIT project drew heavy criticisms from civil rights organizations[70] that highlighted the extremely vague and encompassing proposals for delegating tasks of internet filtering and monitoring to private companies.

Already since the mid-2000s, the EU funded various Internet contact points for the takedown of content as part of the EU Safer Internet programme, which mainly focus on child sexual abuse. This Programme officially already addressed material that is "celebratory, trivializing or inhumane representations of violence [and] material inciting violence for racial or national reasons and glorifying war, propaganda material of unconstitutional organisations."[71] Moreover, the EU Safer Internet Program was intended as a means for private sector organisations to take responsibility and engage with civil society in supporting the police and ensuring a swift takedown of content. Yet instead of clarifying the legal basis or the precise partnership model for such kind of PPPs for content controls, the current focus on online terrorist activities has led to a further period of experimentation with new initiatives such as the IRU, where mutual responsibilities and risks remain unclear.

Conclusion

This article has aimed to provide a nuanced, more focused, yet nonetheless critical reading of PPPs for cybersecurity. To begin with, it is clearly necessary to sharpen our conceptual language and to map the diversity of public-private interactions with regard to the complex notion of cybersecurity. The resulting heuristic typology showed, firstly, that *partnerships* only constitute one part – albeit a key one - of the wider governance processes in this field. In particular, it is helpful to distinguish general policy

[66] https://wiki.openrightsgroup.org/wiki/Counter_Terrorism_Internet_Referral_Unit
[67] http://www.ft.com/intl/cms/s/0/b5b03bb4-a87b-11e3-b50f-00144feab7de.html
[68] https://edri.org/european-internet-forum-untransparent-and-dangerous/
[69] http://www.cleanitproject.eu/about-the-project/
[70] https://edri.org/CleanIT-evaluation/
[71] http://www.fsm.de/hotline

coordination and shared rule-setting for cybersecurity between public and private actor, which may be termed co-regulation, from other forms of cooperation that are rather focused on implementation or operational tasks, such as information exchange and mutual assistance with regard to specific threats. Secondly, the proposed typology underlined the diversity of private stakeholders or communities of practice that contribute to cybersecurity at different technical or logical levels. While it is obvious that owners of critical information infrastructures differ from IT security companies or internet service providers, it has been instructive to compare these different communities across the varied task of public-private interactions for cybersecurity. Such a crosscutting overview underlines that PPPs for cybersecurity often remain at the level of rhetoric and do not correspond to the interest of many private entities. Due to a variety of conflicting interest, blame shifting and cost considerations, one can rather see a trend to more regulatory governance, which is a familiar feature from other economic sectors. Overall, the heuristic typology helped to categorise and differentiate different forms of PPPs for cybersecurity, and to formulate some basic expectations about their prospects, obstacles and possible normative concerns.

The second empirical part of this article applied this heuristic framework about PPPs for cybersecurity to the case of the EU. At the technical and infrastructural levels, we could identify an extension of consultation and co-regulation processes under the leadership of ENISA, whereas broader and more operational notions of PPPs for cybersecurity revealed their limits. Aside from the discontinuation of the so-called E3PR public private partnership for resilience, CERTs have rather moved in the direction of stand-alone *public* capacities for operational cybersecurity. However, the activities of EUROPOL demonstrate that other forms public-private cooperation and partnership for cybersecurity are expanding fast. In particular, the areas of information exchange on illegal content, as undertaken via the new Internet Referral Unit, and of operational assistance with regard to cybercrimes and –threats, as undertaken via the EC3, are currently ill understood.

While one can refer to a wider a debate on the problems of "voluntary" content control, or filtering, on the internet, we have almost no insights into other forms of PPPs for addressing cybercrimes. The mentioned J-CAT Task Force in the EC3 is explicitly designed to take on criminal prosecutions, but also regularly exchanges information with private actors. This underpins the recent statement in the European Agenda on Security, where PPPs are linked with the ambition to develop a "new approach to law enforcement in the digital age" ([20], 20). But despite its evident sensitivity, this "new approach" is nowhere debated in public and rather emerges from diffuses practice of security authorities, supported by private companies that have a direct commercial interest in touting their security expertise and products. While the unavoidability of such collaboration is persistently repeated, it is entirely unclear whether this is actually the case or whether this new approach masks shifts in law enforcement operation and collaboration that would otherwise be impossible.

In sum, flexible and operational PPPs for cybersecurity may have their constructive uses, such as in the case actions against transnational botnets, but the generally ill-defined forms of cooperation should us give pause – even if this article has sought to provide some more focus on the use of the term PPP. One fundamental problem is that the terms 'cyber' and 'security' can be defined to encompass most areas of human life. Therefore, it needs to be spelt out more precisely how PPPs for cybersecurity can be

combined and balanced with other normative principles on transparency, accountability, privacy and other civil and human rights that the EU officially endorses with regard to internet governance [102, 103].

In particular, many of the highlighted developments and initiatives for PPPs can be seen as piecemeal policy developments in relation to different crises, perceived security threats and stakeholder communities. On the one hand, the proposed typology underlines the use for a functional differentiation and tailored instruments for different aspects of cybersecurity. On the other hand, it remains essential for public authorities to keep a wider perspective on the overarching orientation, attribution of responsibilities and legitimate bases for security provision. This concerns, for instance, more hidden, but dynamic developments within professional communities and specialised agencies, as in the case of the EC3.

Aside from general normative debates, we need deeper operational insights into operational cybersecurity PPPs to disentangle the respective power-relations and problems. Conventional PPPs often include contractual arrangements on profit and economic risk sharing, while there are wider debates on appropriate standards for public accountability. In the area of cybersecurity, other forms of risks and responsibilities beyond timely construction or reliable service provision have to be considered. Governments are also increasingly able to exert pressure to obtain 'voluntary' cooperation from business, as illustrated in the controversial area of content control, where various commentators suspect a deliberate blame-shifting strategy of public actors [104]. But when dealing with new or advanced cyber threats, public actors often enter these partnerships as the weaker partner, reliant on specialised IT companies to define the level of vulnerability and appropriate countermeasures. The mentioned Memoranda of Understanding of the EC3 can provide a focal point to test this assumption, as well as to discern the solidity of public criminal prosecution in pragmatic cooperation networks. These memoranda and other related contractual arrangement for PPPs for cybersecurity should be made public as far as possible, which – in light of their general framework nature – should be possible without endangering specific operations against cyber threats. Finally, we would argue that the proposed typology may also be applied beyond the case of the EU, and prepare the ground for more systematic and comparative analyses of appropriate governance frameworks for public private interactions and partnerships for cybersecurity.

References

1. Eriksson, J., & Giacomello, G. (2009). Who controls the internet? Beyond the obstinacy or obsolescence of the State. *International Studies Review, 11*(1), 205–230.
2. Radu, Roxana, Jean-Marie Chenou, and Rolf H Weber. 2014. *The evolution of global internet governance: principles and policies in the making*. Vol. 56: Springer Science & Business Media.
3. Mueller, M., Schmidt, A., & Kuerbis, B. (2013). Internet security and networked governance in international relations. *International Studies Review, 15*(1), 86–104.
4. Von Solms Rossouw, and Johan Van Niekerk. 2013. "From information security to cyber security." *Computers & Security* 38:97–102.
5. Tropina, Tatiana. 2015. "Public–Private Collaboration: Cybercrime, Cybersecurity and National Security." In *Self-and Co-regulation in Cybercrime, Cybersecurity and National Security*, 1–41. Springer.

6. Min, K.-S., Chai, S.-W., & Han, M. (2015). An International Comparative Study on Cyber Security Strategy. *International Journal of Security and Its Applications, 9*(2), 13–20.
7. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs, 92*(1), 43–62.
8. Dunn-Cavelty, M., & 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.
9. van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society, 12*(2), 197–208.
10. Bevir, M. (2014). The Rise of Security Governance. In M. Bevir, O. Daddow, & I. Hall (Eds.), *Interpreting Global Security,* (pp. 17–34). London: Routledge.
11. Hameiri, Shahar, and Lee Jones. 2015. Governing Borderless Threats: Non-traditional Security and the Politics of State Transformation: Cambridge University Press.
12. Nance, M., & Cottrell, P. (2014). A turn toward experimentalism? Rethinking security and governance in the twenty-first century. *Review of International Studies, 40*(02), 277–301. doi:10.1017/S026021051300017X.
13. Crawford, A. (2006). Networked governance and the post-regulatory state? Steering, rowing and anchoring the provision of policing and security. *Theoretical Criminology, 10*(4), 449–479.
14. Ehrhart, H.-G., Hegemann, H., & Kahl, M. (2014). Putting security governance to the test: conceptual, empirical, and normative challenges. *European Security, 23*(2), 119–125.
15. Kennedy, David. 2016. *A World of Struggle: How Power, Law, and Expertise Shape Global Political Economy: Princeton University Press*.
16. Christou, G., & Simpson, S. (2006). The Internet and public–private governance in the European Union. *Journal of Public Policy, 26*(01), 43–61.
17. Procedda, M. (2014). Public-Private Partnerships: A soft approach to cybersecurity? Views from the European Union. In G. Giacomello (Ed.), *Security in Cyberspace: Targeting Nations, Infrastructures, Individual*. New York, London: Bloomsbury Academic.
18. Fahey, Elaine. 2014. "EU's Cybercrime and Cyber-Security Rulemaking: Mapping the Internal and External Dimensions of EU Security, The." *Eur. J. Risk Reg.*:46.
19. EU. 2013. "Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace " *JOIN(2013) 1 final* http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf.
20. European Commission (2015). The European Agenda on Security. *COM, 2015*, 185 .http://eur-lex.europa.eu/legal-content/en/HIS/?uri=celex%3A52015DC0185
21. Grimsey, Darrin, and Mervyn Lewis. 2007. Public private partnerships: The worldwide revolution in infrastructure provision and project finance: Edward Elgar Publishing.
22. Schneider, A. L. (1999). Public-private partnerships in the US prison system. *American Behavioral Scientist, 43*(1), 192–208.
23. Bovaird, T. (2004). Public–Private Partnerships: from Contested Concepts to Prevalent Practice. *International Review of Administrative Sciences, 70*(2), 199–215. doi:10.1177/0020852304044250.
24. Hodge, G. A., & Greve, C. (2007). Public–private partnerships: an international performance review. *Public Administration Review, 67*(3), 545–558.
25. Reynaers, A.-M., & De Graaf, G. (2014). Public Values in Public–Private Partnerships. *International Journal of Public Administration, 37*(2), 120–128.
26. Forrer, J., Kee, J. E., Newcomer, K. E., & Boyer, E. (2010). Public–private partnerships and the public accountability question. *Public Administration Review, 70*(3), 475–484.
27. Willems, T., & Van Dooren, W. (2011). Lost in diffusion? How collaborative arrangements lead to an accountability paradox. *International Review of Administrative Sciences, 77*(3), 505–530.
28. Hodge, Graeme A, and Carsten Greve. 2005. *The challenge of public-private partnerships: Learning from international experience*: Edward Elgar Publishing.
29. European Commission. 2004. "Green paper on public-private partnerships and community law on public contracts and concessions." *COM (2004) 327 final*.
30. United Nations Economic Commission for Europe. 2008. "Guidebook on promoting good governance in public private partnerships." *ECE/CECI/4*.
31. Van, d. H., Martijn, L. B., Lember, V., Petersen, O. H., & Witz, P. (2015). *National varieties of Public–Private Partnerships (PPPs): A comparative analysis of PPP-supporting units in 19 European countries* (pp. 1–20). Research and Practice: Journal of Comparative Policy Analysis.
32. Roumboutsos, Athena. 2015. *Public Private Partnerships in Transport: Trends and Theory*: Routledge.

33. Linder, S. H. (1999). Coming to terms with the public-private partnership a grammar of multiple meanings. *American Behavioral Scientist, 43*(1), 35–51.
34. Bovis, C. H. (2015). Risk in Public-Private Partnerships and Critical Infrastructure. *European Journal of Risk Regulation, 6*(2).
35. Hans, V. D., Sarmento, J. M., & Renneboog, L. (2016). Anatomy of public-private partnerships: their creation, financing and renegotiations. *International Journal of Managing Projects in Business, 9*(1), 94–122.
36. Van, D. H., Martijn, & Verhoest, K. (2016). The challenge of using standard contracts in public–private partnerships. *Public Management Review, 18*(2), 278–299.
37. Brinkerhoff, D. W., & Brinkerhoff, J. M. (2011). Public–private partnerships: perspectives on purposes, publicness, and good governance. *Public Administration and Development, 31*(1), 2–14.
38. Bovis, Christopher. 2013. Public-private Partnerships in the European Union: Routledge.
39. Gómez-Barroso, J. L., & Feijóo, C. (2010). A conceptual framework for public-private interplay in the telecommunications sector. *Telecommunications Policy, 34*(9), 487–495.
40. Braman, S. (2011). The Framing Years: Policy Fundamentals in the Internet Design Process, 1969–1979. *The Information Society, 27*, 295–310.
41. Townes, M. (2012). The spread of TCP/IP: How the Internet became the Internet. *Millennium-Journal of International Studies, 41*(1), 43–64.
42. LaRose, R., Bauer, J. M., DeMaagd, K., Chew, H. E., Ma, W., & Jung, Y. (2014). Public broadband investment priorities in the United States: an analysis of the broadband technology opportunities program. *Government Information Quarterly, 31*(1), 53–64. doi:10.1016/j.giq.2012.11.004.
43. Narayanan, A., Jain, A., & Bowonder, B. (2005). Providing rural connectivity infrastructure: ICT diffusion through private sector participation. *International Journal of Services, Technology and Management, 6*(3–5), 416–436.
44. ENISA. 2011a. "Cooperative Models for Effective Public Private Partnerships." *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/copy_of_desktop-reserach-on-public-private-partnerships/at_download/fullReport*
45. Héritier, A. (2001). Market integration and social cohesion: the politics of public services in European regulation. *Journal of European Public Policy, 8*(5), 825–852. doi:10.1080/13501760110083536.
46. Graz, Jean-Christophe, and Andreas Nölke. 2007. Transnational private governance and its limits: Routledge.
47. Harcourt, A. (2013). Participatory Gains and Policy Effectiveness: The Open Method of Co-ordination Information Society. *JCMS: Journal of Common Market Studies, 51*(4), 667–683. doi:10.1111/jcms.12022.
48. Börzel, T. (2010). European governance: negotiation and competition in the shadow of hierarchy. *JCMS: Journal of Common Market Studies, 48*(2), 191–219.
49. Wagner, B. (2014). The politics of internet filtering: The United Kingdom and Germany in a comparative perspective. *Politics, 34*(1), 58–71.
50. Wiater, P. (2015). On the notion of" Partnership" in Critical Infrastructure Protection. *European Journal of Risk Regulation, 6*(2), 255–262.
51. Bauer, J. M. (2010). Changing roles of the state in telecommunications. *International Telecommunications Policy Review, 17*(1).
52. European Commission. 2013. "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 final* http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666.
53. Marsden, Christopher T. 2011. *Internet co-regulation: European law, regulatory governance and legitimacy in cyberspace*: Cambridge University Press.
54. Tropina, T., & Callanan, C. (2015). *Self-and Co-regulation in Cybercrime, Cybersecurity and National Security*. Heidelberg: Springer.
55. Bendiek, A., & Porter, A. L. (2013). European Cyber Security Policy within a Global Multistakeholder Structure. *European Foreign Affairs Review, 18*(2), 155–180.
56. Carr, M. (2015). Power Plays in Global Internet Governance. *Millennium - Journal of International Studies, 43*(2), 640–659. doi:10.1177/0305829814562655.
57. Chenou, J.-M. (2014). From Cyber-Libertarianism to Neoliberalism: Internet Exceptionalism, Multi-stakeholderism, and the Institutionalisation of Internet Governance in the 1990s. *Globalizations, 11*(2), 205–223.
58. Cavelty, D., & Myriam (2013). From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse. *International Studies Review, 15*(1), 105–122.

59. Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155–1175.
60. Wagner, Ben. forthcoming. "Constructed "Cyber" Realities & International Relations Theory. ." In *Technology and International Relations Theory*, edited by R Marlin-Bennett and J. P. Singh. Cambridge: CUP.
61. Schmidt, A. (2014). Open Security. Contributions of Networked Approaches to the Challenge of Democratic Internet Security Governance. In R. Radu, J.-M. Chenou, & R. H. Weber (Eds.), *The Evolution of Global Internet Governance* (pp. 169–187). Berlin Heidelberg: Springer.
62. Choucri, N., & Clark, D. D. (2012). Integrating Cyberspace and International Relations: The Co-Evolution Dilemma. In *Explorations in Cyber-International Relations: Who Controls Cyberspace?* Cambridge, MA: MIT.
63. DeNardis, L. (2012). Hidden levers of Internet control: An infrastructure-based theory of Internet governance. *Information, Communication & Society, 15*(5), 720–738.
64. Mathew, Ashwin Jacob. 2014. *Where in the World is the Internet? Locating Political Power in Internet Infrastructure*. http://gradworks.proquest.com/3685949.pdf: University of California, Berkeley.
65. DeNardis, Laura. 2014. *The global war for internet governance:* Yale University Press.
66. Ruiz, Jeanette B, and George A Barnett. 2014. "Who owns the international Internet networks?" Journal of International Communication 21 (1):38–57.
67. Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610–613.
68. August, T., & Tunca, T. I. (2011). Who should be responsible for software security? A comparative analysis of liability policies in network environments. *Management Science, 57*(5), 934–959.
69. Brown, Ian, and Christopher T Marsden. 2013. *Regulating code: Good governance and better regulation in the Information Age*: MIT Press.
70. Edwards, Benjamin, Michael Locasto, and Jeremy Epstein. 2014. "Panel Summary: The Future of Software Regulation." Proceedings of the 2014 workshop on New Security Paradigms Workshop, http://dl.acm.org/citation.cfm?id=2683478.
71. Kleinschmidt, Broder. 2010. "An International Comparison of ISP's Liabilities for Unlawful Third Party Content." *International Journal of Law and Information Technology*:eaq009.
72. Rowe, Brent, and Dallas Wood. 2013. "Are Home Internet Users Willing to Pay ISPs for Improvements in Cyber Security?" In *Economics of Information Security and Privacy III*, 193–212. Springer.
73. Usman, S. H. (2013). A review of responsibilities of internet service providers towards their customer network security. *Journal of Theoretical and Applied Information Technology, 49*(1), 70–78.
74. Van Eijk Nico. 2013. "Duties of care on the Internet." In *The Secure Information Society*, 57–81. Springer.
75. Clark, David, Thomas Berson, and Herbert S Lin. 2014. *At the Nexus of Cybersecurity and Public Policy:: Some Basic Concepts and Issues*: National Academies Press.
76. Cohen-Almagor, R. (2015). Internet architecture, freedom of expression and social responsibility: critical realism and proposals for a better future. *Innovation: The European Journal of Social Science Research, 28*(2), 147–166.
77. Horten, Monica. 2015. "The Policy Challenge of Content Restrictions: How Private Actors Engage the Duties of States." *Media@LSE Working Paper* 34 (http://www.lse.ac.uk/media@lse/research/mediaWorkingPapers/pdf/WP34-FINAL.pdf).
78. Parti, K., & Marin, L. (2013). Ensuring freedoms and protecting rights in the governance of the Internet: a comparative analysis of blocking measures of illegal Internet content and the liability of ISPs. *Journal of Contemporary European Research, 9*(1), 138–159.
79. August, T., August, R., & Shin, H. (2014). Designing user incentives for cybersecurity. *Communications of the ACM, 57*(11), 43–46.
80. Camp, L. J. (2011). Reconceptualizing the role of security user. *Daedalus, 140*(4), 93–107.
81. Hare, Forest. 2010. "The interdependent nature of national cyber security: motivating public action for a private good." PhD, George Mason University (http://digilib.gmu.edu:8080/dspace/bitstream/1920/6312/1/Hare_dissertation_2010.pdf).
82. Kaijankoski, Eric A. 2015. Cybersecurity Information Sharing Between Public Private Sector Agencies. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA620766: DTIC Document.
83. Suter, M. (2007). Improving information security in companies: How to meet the need for threat information. In M. D. Cavelty, V. Mauer, & S. F. Krishna-Hensel (Eds.), *Power and Security in the Information Age: Investigating the Role of the State in Cyberspace, Aldershot: Ashgate* (pp. 129–150). Aldershot: Ashgate.

84. Bauer, J. M., JG, M., & Eeten, V. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy, 33*(10), 706–719.
85. Dourado, E., & Castillo, A. (2015). *"Information Sharing": No panacea for American cybersecurity challenges*. Mercatus Center Policy Paper: George Mason University http://mercatus.org/publication/information-sharing-no-panacea-american-cybersecurity-challenges.
86. Nolan, A. (2015). Cybersecurity and Information Sharing: Legal Challenges and Solutions. *Congressional Research Service*, 7–5700 http://a51.nl/sites/default/files/pdf/R43941.pdf.
87. Kesan, J. P., & Hayes, C. M. (2015). Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals. *Michigan State Law Review, 2014*(5), 1475.
88. Rosenzweig, Paul. 2011. Cybersecurity and Public goods. The Public/Private "Partnership". In *Emerging Threats in National Security and Law*, edited by Peter Berkowitz. Stanford: Hoover institution, Stanford University.
89. Prince, Daniel, and Nick King. 2013. "Small business cyber security workshop 2013: towards digitally secure business growth." http://eprints.lancs.ac.uk/65265/.
90. Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cyber crime on the financial sector. *Computers & Security, 45*, 58–74.
91. Brown, I., & Cowls, J. (2015). *Check the web: assessing the ethics of politics of policing the internet for extremist material*. Voxpol: Report http://voxpol.eu/category/publications/vox-pol-publications/.
92. European Union (2013). Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 Text with EEA relevance. *OJ L, 165*, 41–58.
93. ENISA. 2011b. *Cooperative Models for Effective Public Private Partnerships. Desktop Research Report*. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/copy_of_desktop-reserach-on-public-private-partnerships/at_download/fullReport ENISA.
94. Commission of the European Communities. 2009. Communication from the Commission..on Critical Information Infrastructure Protection. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". COM(2009) 149 final.
95. Irion, K. (2013). The Governance of Network and Information Security in the European Union: The European Public-Private Partnership for Resilience (EP3R). In J. Krüger, B. Nickolay, & S. Gaycken (Eds.), *The Secure Information Society* (pp. 83–116). London: Springer.
96. ENISA. 2015. "EP3R 2009–2013 Future of NIS Public Private Cooperation." (https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/ep3r-2009-2013/at_download/fullReport).
97. Morgus, Robert, Isabel Skierka, Mirko Hohmann, and Tim Maurer. 2015. "National CSIRTs and Their Role in Computer Security Incident."
98. RAND Europe. 2012. "Feasibility Study for a European Cybercrime Centre." *http://www.rand.org/pubs/technical_reports/TR1218.html*.
99. Reitano, T., Oerting, T., & Hunter, M. (2015). Innovations in International Cooperation to Counter Cybercrime: The Joint Cybercrime Action Taskforce. *The European Review of Organised Crime, 2*(2), 142–154.
100. General Secretariat of the Council. 2015. "Friends of the Presidency Group on Cyber Issues." *15059/15*.
101. Council of the European Union. 2015. "EU Internet Referral Unit at Europol - Concept note." *7266/15*.
102. European Commission. 2012. "Internet Policy and Governance Europe's role in shaping the future of Internet Governance." *COM/2014/072 final*
103. Wagner, Ben, Kirsten Gollatz, and Andrea Calderaro. 2014. "Internet & Human Rights in Foreign Policy: comparing narratives in the US and EU Internet Governance agenda." *Robert Schuman Centre for Advanced Studies Research Paper No. RSCAS* 86.
104. Walker, C., & Conway, M. (2015). Online terrorism and online laws. *Dynamics of Asymmetric Conflict, 8*(2), 156–175. doi:10.1080/17467586.2015.1065078.