Crime Law Soc Change
DOI 10.1007/s10611-016-9652-4

'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers

Helena Carrapico[1] · **Benjamin Farrand**[2]

Abstract The protection of cyberspace has become one of the highest security priorities of governments worldwide. The EU is not an exception in this context, given its rapidly developing cyber security policy. Since the 1990s, we could observe the creation of three broad areas of policy interest: cyber-crime, critical information infrastructures and cyber-defence. One of the main trends transversal to these areas is the importance that the private sector has come to assume within them. In particular in the area of critical information infrastructure protection, the private sector is seen as a key stakeholder, given that it currently operates most infrastructures in this area. As a result of this operative capacity, the private sector has come to be understood as the expert in network and information systems security, whose knowledge is crucial for the regulation of the field. Adopting a Regulatory Capitalism framework, complemented by insights from Network Governance, we can identify the shifting role of the private sector in this field from one of a victim in need of protection in the first phase, to a commercial actor bearing responsibility for ensuring network resilience in the second, to an active policy shaper in the third, participating in the regulation of NIS by providing technical expertise. By drawing insights from the above-mentioned frameworks, we can better understand how private actors are involved in shaping regulatory responses, as well as why they have been incorporated into these regulatory networks.

Keywords Regulatory capitalism · Network governance · Network information security · Internet · Regulation

✉ Helena Carrapico
h.farrand-carrapico@aston.ac.uk

[1] Aston University, Birmingham, UK

[2] University of Warwick, Coventry, UK

Published online: 11 October 2016

Introduction

Despite being one of the most recent fields of European Union (EU) governance, Network and Information Security (NIS) has also become one of its key priorities. NIS, briefly put, ensures the security of computer networks operating within critical infrastructures such as waste management systems and electricity grids, and the data they contain, through ensuring the resilience of those systems to attacks. The protection of networks and information systems has become essential in a society that is as connected and as dependent on technology as the European one – indeed, the European Commission considers the Internet and digital communications to be "the backbone" of social and economic prosperity, with NIS being the armour preventing it from breaking (Commission, 2014). The recent examples of cyber attacks on the Janet Computer Network (December 2015) and TalkTalk (October 2015) are representative of the challenges posed to operators of Internet-based services, now generally understood by the EU to constitute a form of Critical Information Infrastructure (CII). In the case of the Janet Computer Network attack, British academic institutions found their internal and external network access brought down by a concerted Distributed Denial of Service attack, making university network servers inaccessible [1]. In the case of TalkTalk, an Internet Service Provider offering high-speed broadband Internet access, its servers were not only attacked, making websites slow to respond, but a significant volume of consumer data, including unencrypted personal information, was also accessed and allegedly shared online [2]. The cost of this intrusion, according to some estimates, could reach as high as £60 million, and has resulted in the loss of 100,000 subscribers [3]. Given that approximately 78 % of EU citizens actively use the Internet [69], the breakdown of Internet communications presents significant economic costs, and the unauthorised access to personal data may pose both economic and social costs, including loss of confidence in the security of online transactions [4]. Yet, given that these infrastructures, whether in the form of Internet access providers such as Virgin Media or the Spanish Telefónica S.A. or online service providers such as eBay, Google or Facebook (see [5] for more on this distinction), known collectively as Internet service providers, are privately operated, how best to ensure their security? The dominant view, at least in the EU, is that this is best achieved by bringing in the technical knowledge and expertise of the private actors themselves; after all, who better to identify the challenges that market operators face than those market operators themselves? Within the context of liberalisation and privatisation, as the State has stepped back from the provision of goods and services, the private sector has filled this ostensible gap, and is perceived as being best placed to identify and respond to regulatory challenges.

The present article aims to contribute to the topic of this special issue on how private actors, working in non-private military and security fields, are participating in security governance, by exploring the case study of Internet service providers. As mentioned in the editorial (Bures and Carrapico, this issue), there is a clear gap in the literature in terms of exploring the function and the extent to which private companies, whose main activity is not related to security, are involved in security governance. The present article wishes to contribute to reducing such gap by asking how Internet service providers have been incorporated into and have contributed to shaping the governance of Network and Information Security in the EU. The article argues that Regulatory

Capitalism and Network Governance frameworks can contribute to answering this research question by bringing to light how current economic theories based on liberalisation and privatisation have led to the normalisation of a rationale according to which the private sector should be further involved in the regulatory process, as it is associated, not only to a higher degree of efficiency, but also to a greater level of expertise and knowledge. Such a rationale has resulted in the delegation of regulatory functions to independent bodies, as well as the transfer of the provision of goods and services to the private sector. However, this article argues that there has been a further important shift that has led the private sector working in the area of NIS- related critical information infrastructures to evolve along the following three stages: 1) Private actor h as a passive role as object of regulation; 2) Private actor becomes responsible for adopting regulation; 3) Private actor becomes an active participant in the shaping of that regulation (please see Tables 1 and 2 for further detail).

The authors propose to pursue this argument by, firstly, undertaking documentary analysis to uncover how the role of the private sector is being framed in the area of NIS, and, secondly, by using process tracing to map the evolution of the private sector role along the above-mentioned three stages and identify key turning points.[1] The article starts by discussing the theoretical frameworks of Regulatory Capitalism and of Network Governance, which it then uses to guide us through the evolution of public- private relations in NIS. This evolution is the object of analysis in the second section of the article, which uses the above-mentioned NIS 3 stage approach to understand how private actors in this field have shifted from being framed as victims in need of protection to being considered as actors responsible for adopting regulation, and in a final stage to being seen as participating in the shaping of such regulation. In order to further clarify the dynamics at play within this last stage, the third section focuses on the specific case study of the Telecoms Package and how private actors in NIS have become actively involved in shaping regulatory standards. The final section of the article explores how this governance trend has become further accentuated with an expansion of the role of private actors and of the definition of critical information infrastructures.

Conceptualising the role of private actors in network and information security regulation

As mentioned in the introduction, the article seeks to understand the growing role of the private sector within Network and Information Security (NIS) and its increased influence as policy-shapers, reconceptualised through the lenses of Regulatory Capitalism [6, 12, 13] and of Network Governance [14]. Regulatory Capitalism provides a general framework for understanding the current forms of governance in NIS, by highlighting

[1] We use process tracing here in an interpretive sense; not as a means of identifying causal mechanisms that explain outcomes [8, 9], but as a means of tracing the development of keys ideas and themes by analysing the meanings that actors ascribe to their actions and policies ([10], p. 24). In the way that Schimmelfennig has used process tracing methods to analyse the way that the conceptualisation and internalisation of liberal democracy impacted upon the way in which enlargement decisions were taken by the former communist Member States [11], this article seeks to understand how conceptualisations of how best to regulate and internalised understandings of the expertise held by private sector actors then influences NIS-focused regulatory decisions taken by the Commission.

Table 1 The transformation of governance and the nature of regulatory capitalism (source: [6])

	Laissez Faire capitalism (1800s- 1930s)	Welfare capitalism (1940s- 1970s)	Regulatory capitalism (1980s-)
Steering	Business	State	State and Agencies
Rowing	Business	State	Business
NIS Stages	0	0	1 and 2

the increased role of the private sector in the State/ Private sector division of labour, and by pointing out the resulting reliance on businesses' expertise. Network Governance complements Regulatory Capitalism by conceptualising the growing influence of the private sector as policy shapers and by articulating the existing relations between public and private actors (for more on Public Private partnerships see Bures, this edition, and Bossong and Wagner, this edition).

When 'neoliberal' economic thought became a mainstream approach to economics at the end of the 1970s and beginning of the 1980s, Western governments quickly moved in the direction of cuts to public spending and deregulation, underscored by a belief that the private sector was best placed to achieve the market efficiencies that such an understanding of economic activity entailed. For the purposes of this article, we consider that Neoliberalism is a political economy theory that proposes that individuals' interests are more efficiently achieved in a context of free markets, free trade, strong private property rights and reduced State intervention [15]. Since the 1980s, efficient governance has become intimately tied with privatisation and de-regulation [16]. As argued by Vogel, however, the *theory* of Neoliberalism is rather different from the *practices* of Neoliberalism (1996), which have also been described as 'actually existing neoliberalism' [17, 18]. In fact, rather than the expected deregulation and retreat of the state resulting from this paradigm shift, we have observed a reregulation process, which Gilardi [13], Braithwaite [12] and Levi-Faur [6] have described as contrary to the theory of neoliberalism; instead of markets becoming unregulated akin to a laissez-faire approach to economic activity, regulatory bodies and ensuing regulations have in fact proliferated [12, 19]. Given the exponential increase in non-State regulation, these authors consider that we should, instead, refer to this process as Regulatory Capitalism.

In a rather neofunctionalist approach, in order for the free market to function adequately and for privatisation processes to be implemented and overseen, the creation of independent regulatory bodies was perceived as necessary [20]. The latter included regulatory agencies, regulatory networks, and regulatory instruments, such as public-

Table 2 Adapted table on the transformation of governance and the nature of regulatory capitalism (source: [6, 7])

	Laissez Faire capitalism (1800s–1930s)	Welfare capitalism (1940s–1970s)	Regulatory capitalism (1980s-)	Networked regulatory capitalism
Steering	Business	State	State and Agencies	State, Agencies, Business
Rowing	Business	State	Business	Business
NIS Stages	0	0	1 and 2	3

private partnerships [12]. In a study by Braithwaite and Jordana (referred to in [12], p. vii), which looks at 49 countries from 1920 to 2002, we can observe how the number of regulatory agencies being created leaped from 5 per year between the 1960s and the 1980s, to 40 per year in the period between 1994 and 1996. Numerous examples can be provided of this reregulation process. Where quality standardisation and certification is concerned, for instance, most of the industry is now being regulated by international standards. The International Organisation for Standardisation (ISO), an independent non- governmental organisation, creates international standards for goods and services, including things as different as toy safety, waste management, the work of private security services, and critical infrastructure protection. The standards, which are defined by technical committees comprised of industry bodies, research and testing organisations, local and central government, and consumers, are then voluntarily adopted by industry and public bodies in an attempt to keep a competitive edge and boost their reputation [21]. This global shift has led not only to radical changes in the way the State engages with the economy, but also to a major transformation in the way the economy itself is organised [13, 22]. In light of the article's interest in how the private sector is participating in security governance, it is important to discuss the role of regulatory bodies in this reregulation process. As the empirical sections of the article will point out, although the private sector is traditionally not included in the list of regulatory bodies, it has gradually come to take part in the reregulation process, namely through the encouragement of the State and of regulatory agencies.

As mentioned previously, the decision to create regulatory agencies, networks and instruments is related to the perceived need to efficiently pursue a liberalisation and privatisation agenda. The emergence of regulatory agencies is intimately related to two elements: firstly, the State apparatus, which was understood as too dependent on electoral results and varying political interests, was considered to be too politically uncertain to serve as a solid base for economic development [23]. In order to provide a more coherent and continuous approach, which the markets could rely on, it was decided that efficiency could only be achieved in an apolitical context by professional regulators [24]. Secondly, the process of privatisation also led to public demand for regulation of the private sector and its capacity to provide society with goods and services [7]. As a result, regulatory bodies emerged as the ideal operational solution to regulate liberalisation, in a way that is autonomous from the political system. Their main functions are to collect and process information, as well as to produce efficient solutions to practical regulatory problems [25, 26].

Although the degree of efficiency of Neoliberalism has often been questioned [27–29], there is little doubt regarding the hegemonic character of its discourse, with the consequent reregulation having become 1) the norm in most countries; and 2) transversal to most sectors of the economy. As we will see throughout the article, the efficiency of neoliberal discourse was particularly instrumental in the development of new sectors, in particularly technology-intensive sectors such as the NIS, where private actors' input has been prioritised on the basis of their perceived expertise. As announced in the introduction, it allowed for private actors in the field of Network and Information Security, namely Internet Service Providers, to evolve along three stages: 1) Passive role as object of regulation; 2) Actors responsible for adopting and implementing regulation; 3) Active participants in the shaping of that regulation.

Let us start by focusing on the first stage. As Table 1 indicates, Levi-Faur and Braithwaite consider that the economic governance paradigm of the nineteenth century and early twentieth century, which was based on private initiative or laissez-faire, was replaced with the mid-twentieth century State-based regulatory model (named Welfare Capitalism in Table 1). In the latter, the State is both responsible for organising the economy (steering) and for providing citizens with a considerable amount of goods and services (rowing). The role of the private actors in the second model is limited to areas open to private initiative and competition. According to these authors, the Regulatory Capitalism model (from the 1980s onwards) would be a further evolution, where the State maintains the direction of the economy and oversight over the content of produced regulations, delegating powers to independent agencies to implement and enforce those regulations (steering), with the private sector being responsible for a much larger provision of goods and services (rowing). The privatization of traditional State sectors, such as the electric grid or the management of nuclear power plants are good examples of Regulatory Capitalism model changes. This model corresponds to both stages 1 and 2 of our analytical framework. In the first stage, the private sector adopts a passive role as a 'rower' and as an object of regulation by the State and, in the second stage, it becomes responsible for adopting regulation. Although still in the context of a hierarchical relation, where the regulatory adoption has a mandatory character, the private sector begins to emerge as a more active actor.

This re-emergence of the private sector in the regulatory process is interpreted by Braithwaite [7], Bevir and Rhodes [30] and Castells [28] as transforming what used to be, up until the 1970s/1980s, a single actor system of governance into a form of network governance, characterized by the presence of multiple actors with different functions being brought together (see also [31]). Although Regulatory Capitalism authors make substantial references to the growing importance of the private sector, the majority of this body of literature has two limitations: 1) it is mainly focused on regulatory agencies and their geographical and multilevel diffusion [13, 32], and, more importantly, 2) it depicts the private sector as subservient to State or agency regulation. As a result, the role of industry is generally understood as limited to that of a provider of goods and services that requests and implements regulation [7]. As the empirical sections of this article will point out, however, there are sectors of activity, such as NIS, where the private sector is not only rowing, but also steering.

On this basis, the present article aims to contribute to the Regulatory Capitalism literature by proposing that the shift from a regulatory State to regulatory capitalism paved the way for a greater presence of the private sector, not only as a service provider, but also as an actor within the regulatory process itself, including through self-regulation, and through participation in regulatory bodies. As such, the article proposes a new phase to Levi-Faur's conceptualisation of governance and its transformation. As can be seen in Table 2, the authors propose that a fourth phase be introduced to reflect the private sectors' current role in steering regulation. This arrangement corresponds to stage 3 of our analytical framework, where the private sector is an active participant in the shaping of regulation.

This is an idea that already features in the Network Governance literature [14] and that more adequately represents the role of the private sector in the NIS field, an understanding that can complement and expand the Regulatory Capitalism framework as a way for conceptualising governance within the current economic system. Within

this literature, Risse and Börzel [33] analysed current regulation as being the result of four different relations between public and private entities: 1) 'State-led regulation with consultation of the private sector'; 2) 'State delegation of powers to independent agencies and bodies'; 3) 'Co-regulation between the public and private sectors as equal partners'; and 4) 'Private self-regulation that is sanctioned by the State'. In the remainder of the article, we will see that all these different relations between the public and private sectors have existed at some stage within the European governance of NIS, leading to an understanding of a much more active role of the private sector in the production of regulation than that implied in Regulatory Capitalism. In fact, if we apply the insights of the Network Governance literature to Braithwaite's regulatory networks, we can begin to identify what is actually a more hybrid form of governance [34, 35], in which public-private relations are collaborative, rather than competitive. Network Governance also provides some insights into the organisational rationale of these regulatory networks, allowing us to understand how the private sector managed to achieve such a key position within the production of regulation of NIS. The transnational networks are not formed around formal power and institutional design, but rather around technical knowledge and expertise. Control over the expertise is essential to the capacity to exert control over the regulatory process [36]. As a result, depending on the field, expertise could be located within different actors. Within the current economic framework, 'expertise' is closely linked to business practice, based as it is in the belief that private market actors are efficient and best placed to understand their regulatory needs (see for example [37]).

As will be argued throughout the article, in the case of NIS, as in most emerging areas, the State and independent regulatory agencies do not have adequate technical knowledge to regulate this field. In order to protect critical information infrastructures, it is considered necessary to be aware of the most recent cyber threats and how to appropriately respond to them. Even if security is not the main business of a great deal of information and technology companies, such as Internet service providers, they are considered to be better placed to understand, and subsequently minimise the risks within NIS [38]. When Regulatory Capitalism draws insight from Network Governance, it can serve to better understand *how* private actors are involved in regulation of specific sectors, as well as *why* they are brought into these regulatory networks. In the next section of this article, the development of the role of private actors in NIS will be further explored, highlighting the European Commission's developing of NIS policy. In particular, it will demonstrate the shifting perception of the private sector from being potential victims of cyber-attacks, to commercial actors bearing responsibility for the adoption of regulatory standards for system resilience, identified by a regulatory agency.

NIS stages 1, 2 and 3: private actors as objects of regulation, as regulation adopters, and as regulation shapers

Dedicated European Commission efforts in the field of cyber-security and NIS can be traced at least as far back as the 2001 initiative, 'NIS: Proposal for A European Policy Approach', which discussed the protection of networks and information systems in security terms [39]. Prior to 2001, States were presented as being responsible both for implementing Network and Information Security legislation and for combating

criminal activities affecting NIS. Although the private sector was starting to be present in the area, a considerable part of the services was still provided by the public sector. The 2001 Communication, however, marks an important turning point in the division of labour between the public sector and businesses, as it finds a new role for the private sector, more characteristic of the 'regulatory capitalism' model.

Stage 1: the emergence of EU cyber-security and the emphasis upon the private sector

In the 2001 Communication, the Commission states that "security is becoming a key priority because communication and information have become a key factor in economic and societal development" (2001, p. 2). NIS, for the purposes of this Communication, was considered as constituting "the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions" (2001, p. 3). Such actions include the interception of communications data, unauthorised access into a computer system for the purposes of copying, modifying or destroying information, disruptive attacks such as Distributed Denial of Service attacks (DDoS) and the spreading of malware or other forms of virus ([39], pp. 3–4). While, prior to the 2001 initiative, there had been indirect EU concerns over illicit activities taking place online, they were not necessarily conceptualised in terms of 'security' of systems themselves, but instead in terms of combatting 'cybercrime' (see for example [40]). Furthermore, emphasis was placed upon the types of data that may be subject to unauthorised access or use, such as personal or private data [41], resulting in Directive 1995/46/EC on the Protection of Personal Data, and copyrighted works available on the Internet [42], and in Directive 2001/29/EC on Copyright in the Information Society. At the same time, at the international level, states concluded the Council of Europe's Convention on Cybercrime, intended to facilitate a common approach to computer-based crimes such as the illegal access or interception of data, data interference, systems interference and content related offences such as the distribution of materials depicting child abuse, or intellectual property infringements ([43]; see also [44]). Again, however, this Convention focused on the combatting of criminal acts and on the requirement of criminal sanctions, rather than focusing upon attacks on information systems in terms of security and resilience. In this respect, early initiatives in this field view the private sector as largely being the *victims* of such attacks, rather than having a responsibility to anticipate and resist such attacks. Whereas previously, telecommunications networks were operated by the public sector, a liberalised, decentralised market open to competition resulted in "many private operators and service providers [acting…] increasingly on a European and global level" ([39], p. 2). This, the Commission acknowledged, made the regulation of this sector somewhat complex (2001, p. 2), and dependent upon *cooperation* between undertakings (2001, p. 19). While the State was continuing to do the 'steering', the 'rowing' of service provision was being conducted by the private sector; what was needed was regulatory oversight.

Stage 2- from passive to active actors responsible for adopting regulation

In order to facilitate this oversight, the EU established the European Union Agency for Network and Information Security (ENISA) through Regulation No 460/2004 in 2004.

Becoming operational in 2005, ENISA was initially given a mandate to "assist the Commission and the Member States, and in consequence cooperate with the business community, in order to help them meet the requirements of NIS" (Regulation No 460/2004, Article 1(2)). Through this framing in the Regulation, it becomes clear that the Commission views the private sector operators not only as the target for potential cyber-attacks, but in fact as an active stakeholder that should form part of the regulatory structure. Recital 3 of the ENISA Regulation, for example, makes reference to "the huge number of private and public actors that bear their own responsibility". However, it would also appear from the Regulation that the role of private sector actors is predominantly that of passive recipients of information intended to improve their NIS policies; Article 3(c) refers to the role of ENISA in enhancing cooperation between different actors cooperating in NIS through organising consultations with industry and establishing working groups for private sector and consumer bodies. While Recital 24 makes reference to receiving input and expertise from the private sector, the emphasis in Article 3 is upon the use of private sector actors to adopt and diffuse NIS policies, akin to the traditional regulatory capitalism approach.

Stage 3- the development of a multi-stakeholder governance model: from regulation adopters to regulation shapers?

In 2006, the Commission began to lay down the foundations for a larger mandate for ENISA and further legislation in the field of NIS with its Communication 'A Strategy for a Secure Information Society' [45]. The document stated that "the availability, reliability and security of networks and information systems are increasingly central to our economies and to the fabric of society" (2006, p. 3). NIS as currently understood by the Commission expands upon the 2001 Communication definition, while reiterating the emphasis on resilience. NIS is, according to this Communication,

> [T]he ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems ([45], p. 3).

As will be demonstrated through discussion of later Commission initiatives, the need to protect the Internet is hereafter closely associated with issues of growth and economic development as specific security issues; as the Commission states, "ICT is a critical component of innovation and is responsible for nearly 40% of productivity growth […] According to Eurostat, 89% of EU enterprises actively used the Internet in 2004" as did approximately 50 % of EU consumers (2006, p. 5), numbers that had increased by 2013 to 90 % [46] and 81 % respectively [47]. Given the near-ubiquitous use of information systems by both enterprise and individuals, a breach of NIS can result in severe consequences beyond the purely economic, with potential repercussions for other forms of critical infrastructure, such as loss of energy supplies or failure of transport networks (2006, p. 5). Indeed, as Knowles et al. indicate, corporate networks and the Internet increasingly form part of industrial control systems, presenting potential risks to physical industrial systems through the misuse or attack of computer systems [48]. However, and of direct relevance to this paper, the 2006 Commission

Communication proposes a strategy for ensuring NIS that goes beyond the initial discussions in the 2001 Communication and the previously limited role of the private sector under the 2004 ENISA Regulation, through direct interaction and engagement with private stakeholders, based on "dialogue, partnership and empowerment" (2006, p. 6). The Commission views the roles of private and public sectors regarding NIS as complementary, necessitating policies based on multi-stakeholder dialogue (2006, p. 6), facilitating the private sector actors as regulation shapers, rather than 'mere' regulation adopters or diffusers. This would reflect the proposed 'networked regulatory capitalism' phase of Regulatory Capitalism, in which 'steering' is conducted through the cooperation of state, agency and private sector in determining the content of regulation. In this phase, the private sector does not only act as an adopter of regulation, but can also be actively involved in shaping policy responses and the resulting regulation.

In the case of NIS, the effective methods of ensuring the resilience of information systems are considered by the Commission to be through benchmarking of national NIS policies, the identification of best practices, and stakeholder debates on how to use existing regulatory instruments, as well as ensuring private actors work *with* ENISA to collect data on cyber-security incidents (2006, p. 8). Finally, the Commission invited private sector firms to "develop an appropriate definition of responsibilities for software producers and Internet service providers in relation to the provision of adequate and auditable levels of security" (2006, p. 9), leaving the choice of policy definition to these private actors, as well as the choice of whether to engage with this process. This would appear to indicate a shift of the private sector from a victim of cyber-attacks to be protected by national legislation, to a self-regulator with an imposed duty to ensure that it responds effectively to ENISA-identified security threats, and thereafter to an active participant in shaping regulations applicable to NIS. This last shift will be discussed further in the next section.

The telecoms package as a stage 3 case study

The formalisation of the role of private sector actors as one of being actively involved in shaping NIS resilience standards beyond engagement with ENISA, rather than 'merely' adopting and diffusing such standards begins with the passing of Directive 2009/140/EC in November 2009, known as the 'Telecoms Package' (see for example [49]). While previous legislative initiatives, as discussed in the preceding section, focused upon the criminalisation of attacks on information systems, with the Telecoms Package comes both a requirement of system resilience, as well as an active role in regulatory standard-setting. This again demonstrates the usefulness of extending the regulatory capitalism framework from its focus on 'state' (the EU) and 'agency' (ENISA) to include 'business' (private sector ISPs). While a substantial body of the academic discussion on the Telecoms Package has been dedicated to the politics of intellectual property law-making ([49–51] for example), comparatively little attention has been paid to the impact upon NIS. Directive 2009/140/EC (amongst other things) amends Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, inserting two new Articles on the security and integrity of networks and services. Article 13a requires in particular that Member

States ensure that "undertakings providing public communications networks or publicly available electronic communications services take appropriate technical and organisational measures to appropriately manage the risks posed to security of networks and services". Furthermore, under subsection 3, Member States should also ensure that "undertakings providing public communications networks or publicly available electronic communications services notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services".[2]

While Article 13a is addressed to Member States and National Regulatory Authorities (NRAs), giving the appearance that private stakeholders such as ISPs play no role in dictating the terms of regulation or shaping policy in this area, their actual position is not so clear cut. In a Communication on Critical Information Infrastructure Protection (CIIP) published in March 2009, approximately six months before the adoption of the Telecoms Package, the Commission referred to the new regulatory regime as including "new provisions on security and integrity, in particular to strengthen operators' obligations to ensure that appropriate measures are taken to meet identified risks, guarantee the continuity of supply of services and notify security breaches" ([56], p. 3). Reiterating the need to ensure NIS due to the social and economic importance of computer networks for business and individuals and the potential impact of cyber-attacks ([56], p. 4), the Commission admitted the governance problems arising from the need to protect CIIs. While Member States are considered as retaining the ultimate responsibility for defining CII-related policies, "their implementation depends on the involvement of the private sector, which owns or controls a large number of CIIs" ([56], p. 5). The Commission expressed hope that a multi-stakeholder governance model, facilitated by ENISA, could "foster the involvement of the private sector in the definition of strategic public policy objectives as well as operational priorities and measures" ([56], p. 6), linking national policy-making to operational expertise, and putting the private sector at the centre of the regulatory process, 'steering' as well as 'rowing'. The role of ENISA as facilitator is highlighted in the preamble to Directive 2009/140/EC, where it is stated at recital 44 that ENISA "should contribute to the enhanced level of security of electronic communications by, among other things, providing expertise and advice, and promoting the exchange of best practices". ENISA, in order to contribute toward these new policy approaches, was newly empowered under Regulation No 526/2013 to actively engage in the development of policies concerning NIS under Article 2(2), in addition to its coordinating and consultative roles. These policies were to be designed through analysing publicly available NIS

[2] The basis for this obligation can be found in the Communication on Electronic Communications Regulation [52], in which the Commission states that NIS is gaining in importance, and greater efforts to counter security threats were needed "given the significant social and economic impact of illicit activities in this area" ([52], p. 18). In order to achieve the goal of improving the resilience of computer systems, the Commission concluded that "close cooperation between enforcement authorities, network operators and ISPs at national level is also needed" ([53], p. 71), which would be tackled through amendment of the existing telecommunications regulations. The original Directive 2002/21/EC made no mention of network or information security, and neither did the Commission Communication upon which the Directive was based [54]. The decision by the Commission to impose such obligations upon ISPs appears instead to have its origins in the above-stated 2006 Communication, as mentioned explicitly in the Proposal for the Telecoms Package, which states that the NIS-related amendments to Directive 2002/21/EC are "designed to strengthen the resilience of current electronic communications networks and systems" ([55], p. 3).

strategies and promoting their publication, as well as identifying best practices in industry, as indicated in Article 3. To achieve this facilitation of coordinated policy action and identification of best practices, ENISA has set up the Article 13a Expert Group, comprising representatives from the NRAs, as well as "experts working in the electronic communications sector via ENISA's electronic communications reference group" ([57], p. ii). This electronic communications reference group has met three times so far, the first time in Rome in 2013, and most recently in Lisbon in January 2015. While ENISA does not provide a list of members of the reference group, it does nevertheless state that it comprises experts from the national telecoms providers (including mobile and Internet Service providers) [58, 59]. Working through a multi-stakeholder process, ENISA, the NRAs and telecoms providers have developed a single harmonised framework for the interpretation of Article 13a, intended as "a tool *for authorities* supervising the electronic communications sector, to be used as a structure for creating guidance or recommendations for providers" ([57], p. iv). Yet what are these standards based on? Are they 'top-down' standards imposed by NRAs and ENISA? It would appear that the answer to this question is 'no'. Referring back to the 2009 Communication on CIIP, it is understood by the European Union institutions and ENISA that private sector involvement is essential to the creation of a well-functioning NIS regime. As a document published by ENISA in 2012 demonstrates, the standards applied to ensuring information security and integrity are based heavily upon a set of twenty industry standards in use in the EU telecommunications market (2012, p. 4), including ISO 27001 on the governance of information security, used by all respondents to ENISA's surveys and interviews ([60], p. 5). In response to the interview question asking what standard should be used for an EU-wide information security good practice requirement, all respondents answered that it should be based upon the ISO 27001 standard (2012, p. 14). Through the identification of standards of best practice, as well as the perceived position of experts in the field of telecoms, although the Commission has imposed binding legislation upon them, they have nevertheless been able to influence the standards by which the legislation is applied and interpreted by feeding into the multi-stakeholder process. It is likely that the private sector will be as actively involved in such activities in the future; according to ENISA's 2016 Work Programme, it is stated that ENISA will continue to work with NRAs and the private sector to "analyse the national reports […and] identify new trends and develop good practices and lessons learned" ([61], p. 30). Furthermore, ENISA states that it will work with the private sector (in addition to the public sector) to both develop and disseminate recommendations, good practices and new initiatives (2015b, p. 31). In this way, private industry is able to shape both the current NIS policies developed by and applied throughout the EU, as well as being well placed to contribute to their development in the future.

An expansion of the 3rd stage? The current trend towards a more comprehensive role for a larger number of private sector actors in critical information infrastructures

As discussed, the above security and incidence reporting requirements were imposed upon telecoms operators solely, including ISPs. However, as the use of web-based

services such as online document storage, social media tools and databases has become more widespread, so too has the understanding amongst EU institutions that these *online service providers* could also constitute CII, not only the ISPs acting as *access providers*, and should therefore also ensure NIS through resilience to attack. Through this, we see that the Commission's approach to regulation in this field is to draw a larger range and number of private sector stakeholders into this regulatory sphere, based on perceptions of industry know-how, and allowing for these actors to actively 'steer' regulatory standards. In December 2009, just one month after the passing of the Telecoms Package, the Council passed a Resolution reiterating the growing importance of NIS, as well as the importance of collaboration between the private sector and governments. In the Resolution, the Council stated that the multi-stakeholder approach is important in mitigating "identified risks where such an approach delivers added value in helping to ensure a high level of network resilience" ([62], sec. IV(7)) and reiterated the "vital role providers play in providing robust and resilient electronic communication infrastructures to society" (2009, sec. IV(8)). The document proposed the expanding of ENISA's mandate, as well the facilitating of a larger role for the private sectors in NIS protection (2009, sec. VII(6)). Interestingly, the private sector is invited to "continue to work on standardisation of NIS to strive to find harmonised and interoperable solutions" (2009, sec. IX(4)), indicating that the Council perceives the expertise held by private sector actors in their fields of activity to be an efficient and effective means of regulating NIS, reinforcing the position of these private actors as policy-shapers, albeit indirectly through the setting of standards rather than directly influencing legislation.

Cyber-security and NIS forms part of the EU's Digital Agenda, which is part of the Europe 2020 initiative. Europe 2020, shaped by concerns over the significant impact of the Global Financial Crisis upon EU economic growth and stability ([63], p. 6; see also [64]), proposed a number of initiatives intended to restore the EU to economic strength (2010b, p. 8). The 2010 Digital Agenda Communication stated with regard to cyber-security that the "cooperation of relevant actors needs to be organised at global level to be effectively able to fight and mitigate security threats" ([4], p. 17). The Commission stated it would pursue a renewed and reinforced NIS policy, and would "foster multi-stakeholder dialogue and self-regulation of European and global service providers (e.g. social networking platforms, mobile communications providers)" (2010a, pp. 17–18), indicating both that the understanding that private sector actors are best-placed to tackle security threats, allowing for them to be involved in the shaping of cyber-security responses, as well as expanding the focus of NIS efforts from telecoms (i.e. access providers) to online service providers. Pillar III of the Digital Agenda Strategy, named 'Trust and Security' provides a series of actions for the European Commission to undertake, including Action 28: A Reinforced Network and Information Security Policy. This Action included the extending of ENISA's mandate and position as the 'fulcrum' for EU expertise and information exchange, as well as serving as the basis for an additional Action Point 123: a proposed Directive on NIS [65].

The proposed NIS Directive was preceded by the Cyber-security Strategy of the European Union published in February 2013, in which it was again affirmed that cyber-security is seen as a multi-stakeholder effort with a significant role for the private sector ([66], p. 4). In the legislation as proposed, the European Parliament et al. state that the involvement of the private sector in both facilitating resilience in NIS, as well as defining the standards for NIS, is essential. The proposal was intended to:

> Improve preparedness and engagement of the private sector. Since the large majority of network and information systems are privately owned and operated, improving engagement with the private sector to foster cybersecurity is crucial. The private sector should develop, at technical level, its own cyber resilience capacities and share best practices across sectors. (2013, p. 6)

The Commission subsequently released an Impact Assessment, creating "a strong incentive [for public administrators and private actors] to manage and dimension security risks effectively" by imposing a regulatory regime facilitating private stakeholder involvement (67, p. 6). The resulting Proposal indicated that upon consultation with the private sector, as with the Telecoms Package security amendments, standard setting for resilience would be best based upon industry standards, placing the private sector not only in the 'steering' category of the networked regulatory capitalism phase, but at its helm. Recital 32 of the proposed Directive states that the "standardisation of security requirements is a market-driven process. To ensure a convergent application of security standards, Member States should encourage compliance or conformity with specified standards to ensure a high level of security at Union level". The relevant private actors, according to the Proposal, are information society providers as defined by Directives 98/34/EC Article 1(2) and 2000/31/EC Article 2(a), namely "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services", which would cover all Internet services such as Google, Facebook or Twitter, but not the ISPs themselves, as they are already covered by the amendments made to the above-discussed Directive 2002/21/EC (as stated in the proposed Directive Article 1(3). Article 14(1) states that Member States should "ensure that public administrations and market operators take appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations", with Article 16(1) stating that Member States should "encourage the use of standards and/or specifications relevant to networks and information security". These standards would presumably be those used by private actors providing online services.

Indeed, this would appear to be the view of the Commission; in a 'Frequently Asked Questions' document released pertaining to the proposed Directive, the Commission stated that it did not see itself as a standard setting body, instead providing a minimal legislative requirement that would facilitate ENISA to "work with standardisation bodies and all relevant stakeholders to develop technical guidelines and recommendations for the adoption of NIS benchmarks and good practices" [68]. On this basis, a High Level Conference held by the Commission took place on 28 May 2015, with over 200 public and private sector representatives, including representatives from service providers such as Blackberry, Amazon, IBM, Microsoft and Symantec. The purpose was "exploring the way forward regarding the Commission proposal for a Directive laying down measures to ensure a high level of NIS across the Union" [69]. At the time of writing, while the Directive has not yet been formally adopted, there has nevertheless been political agreement between the European Parliament and Council [70] on the Commission's proposal, achieved through an informal trilogue in December 2015 [71]. What is particularly interesting is the way in which the Directive has been revised in trilogue to further establish the role of private sector actors in protecting NIS. While not

legally binding, some of the recitals indicate a clear intent for the regulation of NIS to incorporate the private sector; reiterating that "cooperation between the private and public sector is essential", the Directive specifies that informal cooperation should be encouraged between market operators so as to ensure NIS at Recital 34. Furthermore, ENISA is regarded as having an essential role in disseminating best practices and expertise (Recital 35), and is also specifically tasked with providing advice and guidelines to Member States regarding market-driven standards (Recital 66). The revised Directive provides more concrete definitions of the relevant private actors in Article 3, which as well as including operators of essential services such as airlines (a list of essential services being included in Annex II appended to the Directive), states that it applies to 'digital service providers' (Article 3(11da)), including operators of online marketplaces (Article 3(11e)), online search engines (Article 3(11 g)) and cloud computing services (Article 3(11j)). Again, highlighting the nature of NIS as a sector in which regulatory networks comprising public and private actors are deemed most effective, Article *8a* establishes a Cooperation Group, comprising representatives of the Commission, ENISA and the Member States, which may "invite representatives from the relevant stakeholders to participate in its work". The relevant work, as indicated in Article 8(3), is to include establishing work programmes, as well as exchanging best practices on incident notification, capacity building, training, and research and development, as well as identifying best practices in national NIS practices and policies through periodic evaluations. The role of private actors is significant; whereas Article 14(1) is largely untouched in the revision to the Directive, Article 16(1) on standards is significantly modified, stating that Member States should "encourage the use of European or internationally accepted standards and/or specifications" for NIS, and adding a clause that "ENISA shall elaborate advice and guidelines regarding the technical areas which should be considered in relation to paragraph 1 as well as regarding already existing standards". These standards, as discussed above, constitute those best practices established by existing private actors in these fields. ENISA, as indicated in its 2016 Work Programme, foresees itself as having a guiding and coordinating role in the implementation of the Directive, stating that "ENISA will leverage its existing knowledge and expertise in stakeholder engagement with the public and/or private sector" (2015b, p. 35). The Work Programme refers to ENISA's previous successes in achieving this with regard to other sectors such as the establishment of minimum security measures for smart grids, and that through engagement its existing working groups, can quickly and effectively identify relevant sectoral actors, engage with them on identifying best practices and, subsequently, how best to implement them (2015b, p. 35). This ultimately means that, as with the amendments produced as a result of the Telecoms Package, while private sector actors may not necessarily be dictating the wording of the legislation per se, they will nevertheless be able to shape the regulatory approaches dictated *by* legislation through the use of their industries' standards and best practices, as well as the way in which they will be implemented. The development of the NIS Directive demonstrates that the expansion of role witnessed in the Telecoms Package is not an unusual development in this field, but in fact was the first step in the development of a more holistic approach to NIS protection, incorporating a wider body of private sector actors in the identification and dissemination of industry best practices as regulatory tools

Conclusion

This article has sought to provide a case study in how private actors who are not considered security actors have nevertheless been incorporated into security-related regulatory structures, based on the knowledge and expertise they are perceived to possess. On the basis of the Regulatory Capitalism and Network Governance frameworks, the article has sought to provide a better understanding not only of *how* these private actors become involved in security governance, but also of *why* they are brought into the regulatory structure not only as policy adopters, but also as policy shapers. On the basis of the proposed theoretical framework, the article develops a 3 stage analysis that explores the evolution of the private sector in NIS from objects of regulation, to regulation adopters and, at a later stage, to regulation shapers. This adds to the existing Regulatory Capitalism framework by demonstrating the ways in which private actors can take on an active 'steering' function in regulation by the shaping of regulatory responses, rather than a more passive role of adopting or diffusing regulation (i.e. 'rowing'). The understanding that Internet service providers have technical knowledge and expertise not possessed by the State or regulatory agencies has resulted in technical standards developed by private industry actors being adopted as resilience standards for NIS by bodies such as ENISA; furthermore, through active engagement in working groups and expert committees, these industry actors are able to shape regulatory responses through the coordinated and cooperative identification of best practices that serve as the basis for the EU's resilience strategies. Current developments in this field indicate that this trend is likely to continue, if not accelerate, particularly in areas of technological complexity. The private sector may not serve only to steer the ship; instead, it may determine its ultimate destination.

Acknowledgments The authors of this article would like to sincerely thank the editors of this special issue, as well as the reviewers of this article, for their useful comments, advice and support.

References

1. JISC. (2015). DDoS attack disrupting Janet network [WWW Document]. JISC News. URL https://www.jisc.ac.uk/news/ddos-attack-disrupting-janet-network-08-dec-2015 (Accessed 29 Feb 2016).
2. Gibbs, S. (2015). TalkTalk criticised for poor security and handling of hack attack. The Guardian.
3. Farrell, S. (2016). TalkTalk counts costs of cyber-attack. The Guardian.
4. European Commission. (2010a). A digital agenda for Europe (No. COM(2010) 245 final/2). Brussels.
5. Farrand, B. (2016). The future of copyright enforcement online: intermediaries caught between formal and informal governance in the EU, in: Stamatoudi, I.A. (Ed.), New Developments in EU and International Copyright Law. Kluwer Law International, Alphen aan den Rijn.
6. Levi-Faur, D. (2005). The rise of regulatory capitalism: the global diffusion of a new order. *The Annals of the American Academy of Political and Social Science, 598*, 12–32. doi:10.1177/0002716204272590.
7. Braithwaite, J. B. (2005). Neoliberalism or regulatory capitalism (no. Regnet. *Occasional Paper, 5*.
8. Bennett, A., Checkel, J.T., 2014. Process tracing: from philosophical roots to best practices, in: Bennett, A., Checkel, J.T. (Eds.), Process Tracing: From Metaphor to Analytic Tool. Cambridge University Press, Cambridge, pp. 3–37.

9. George, A.L., Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press, Cambridge, Mass.
10. Hall, P. A. (2013). Tracing the progress of process tracing. European. *Political Science, 12*, 20–30. doi:10.1057/eps.2012.6.
11. Schimmelfennig, F. (2003). The EU, NATO and the integration of Europe: Rules and rhetoric. Cambridge University Press, Camberidge, UK; New York.
12. Braithwaite, J. (2008). Regulatory capitalism: how it works, ideas for making it work better. Edward Elgar, Cheltenham.
13. Gilardi, F. (2008). Delegation in the regulatory state: Independent regulatory agencies in Western Europe. Edward Elgar Publishing Ltd, Cheltenham, UK ; Northampton, MA.
14. Börzel, T. A. (1998). Organizing Babylon - on the different conceptions of policy networks. *Public Administration, 76*, 253–273.
15. Harvey, D. (2007). A brief history of Neoliberalism, New Ed edition. ed. OUP Oxford, Oxford; New York.
16. Fourcade-Gourinchas, M., & Babb, S. L. (2002). The rebirth of the liberal creed: paths to neoliberalism in four countries. *American Journal of Sociology, 108*, 533–579. doi:10.1086/367922.
17. Cahill, D. (2015). The End of Laissez-Faire?: On the Durability of Embedded Neoliberalism. Edward Elgar, Cheltenham, UK.
18. Vogel, S.K. (1996). Freer markets, more rules: Regulatory reform in advanced industrial countries. Cornell University Press, Ithaca.
19. Levi-Faur, D., & Jordana, J. (2005). Globalizing Regulatory Capitalism. *The Annals of the American Academy of Political and Social Science, 598*, 6–9. doi:10.1177/0002716204272612.
20. Haas, E.B. (1968). The uniting of Europe: Political, social and economic forces, 1950–57, 2nd Revised edition edition. ed. Stanford University Press.
21. Ponte, S., Gibbon, P., Vestergaard, J. (Eds.). (2011). Governing through standards: Origins, drivers and limitations, 2011 edition. ed. AIAA, Houndmills, Basingstoke, Hampshire ; New York.
22. Majone, G. (Ed.), (1996). Regulating Europe. Routledge, London.
23. Moe, T. M. (1990). Political institutions: The neglected side of the story. *Journal of Law, Economics, & Organization, 6*, 213–253.
24. Lægreid, P., Verhoest, K. (2010). Introduction: Reforming public sector organizations, in: Lægreid, P., Verhoest, K. (Eds.), Governance of Public Sector Organization: Proliferation, Autonomy and Performance. AIAA, Hampshire, UK.
25. Dehousse, R. (1997). Regulation by networks in the European Community: the role of European agencies. *Journal of European Public Policy, 4*, 246–261.
26. Rittberger, B., Wonka, A. (Eds.). (2012). Agency governance in the EU. Routledge.
27. Bourdieu, P. (1998). The essence of neoliberalism. Le Monde diplomatique.
28. Castells, M. (1996). The rise of the network society: - economy, society, and culture. Blackwell, Oxford.
29. Chomsky, N. (1998). Profits over people: Neoliberalism and the global order. Seven stories Press, U.S., New York.
30. Bevir, M., Rhodes, R.A. (2003). Interpreting British governance. Routledge, London.
31. Lazer, D. (2005). Regulatory capitalism as a networked order: the international system as an informational network. *The Annals of the American Academy of Political and Social Science, 598*, 52–66. doi:10.1177/0002716204272590.
32. Jordana, J., Levi-Faur, D. (2004). The politics of regulation in the age of governance, in: Jordana, J., Levi-Faur, D. (Eds.), The Politics of regulation: Institutions and regulatory reforms for the age of governance. Edward Elgar Publishing Ltd, Cheltenham, UK.
33. Risse, T., Börzel, T.A., 2005. Public-Private Partnerships: Effective and Legitimate Tools of International Governance, in: Grande, E., P, Auly, L.W. (Eds.), Complex sovereignty: Reconstituting Political Authority in the Twenty-First Century. University of Toronto Press, Toronto.
34. Calliess, G.-P., Zumbansen, P.C. (2010). Rough consensus and running code: A theory of transnational private law. Hart Publishing, Oxford.
35. Picciotto, S. (2006). Regulatory networks and global governance. University of London, Institute of Advanced Legal Studies.
36. Cohen, E. (2011). Assessing the impact of the global financial crisis on transnational financial law and regulation. Finnish Yearbook of International Law 22, 51–84.
37. Culpepper, P.D. (2011). Quiet Politics and Business Power: Corporate Control in Europe and Japan. Cambridge University Press, Cambridge.
38. Farrand, B., & Carrapico, H. (2013). Networked Governance and the Regulation of Expression on the Internet: The Blurring of the Role of Public and Private Actors as Content Regulators. *Journal of Information Technology & Politics, 10*, 357–368.

39. European Commission. (2001). Network and Information security: proposal for A European policy approach (No. COM(2001) 298 final). Brussels.
40. Porcedda, M.G. (2011). Translantic approaches to cybersecurity and cybercrime, in: Pawlak, P. (Ed.), The EU-US Security and Justice Agenda in Action. Chaillot Papers.
41. European Commission (1990). Protection of individuals in relation to the processing of personal data in the Community and information security (No. COM(90) 314).
42. European Commission. (1995). Green paper: Copyright and related rights in the information Society (No. COM(95) 382 final). European Commission, Brussels.
43. Council of Europe. (2001). Convention on Cybercrime, CETS No. 185, Budapest 23 November 2001.
44. Clough, J. (2012). The Council of Europe Convention on cybercrime: defining `crime' in a digital world. *Criminal Law Forum, 23*, 363–391. doi:10.1007/s10609-012-9183-3.
45. European Commission. (2006). A strategy for a secure information society: - "Dialogue, partnership and empowerment" (No. COM(2006) 251 final). Brussels.
46. Eurostat. (2013). Enterprises with fixed broadband access. Brussels.
47. Eurostat. (2014). Percentage of households who have internet access at home. Brussels.
48. Knowles, W., Prince, D., Hutchison, D., Disso, J. F. P., & Jones, K. (2015). A survey of cyber security management in industrial control systems. *International Journal of Critical Infrastructure Protection, 9*, 52–80. doi:10.1016/j.ijcip.2015.02.002.
49. Reestman, J.-H., & Eijsbouts, W. T. (2009). Internet policy and the European political and legal orders. *European Constitutional Law Review, 5*, 169–172.
50. Coudert, F., & Werkers, E. (2010). *The Aftermath of the Promusicae Case: How to Strike the Balance? Int J Law Info Tech 18*, 50–71. doi:10.1093/ijlit/ean015.
51. Horten, M. (2011). The copyright enforcement enigma: Internet politics and the telecoms package. Palgrave Macmillan, New York.
52. European Commission. (2007a). European electronic communications regulation and markets (12th Report) (No. COM(2007) 155 final). Brussels.
53. European Commission. (n.d). Commission staff working document annex to the European electronic communications regulation and markets (12th Report) (No. SEC(2007) 403). Brussels.
54. European Commission. (2000). Proposal for a directive of the European Parliament and of the council on a common regulatory framework for electronic communications networks and services (No. COM(2000) 393 final). Brussels.
55. European Commission. (2007b). Proposal for a directive amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and services, and 2002/20/EC on the authorisation of electronic communications networks and services (No. COM(2007) 697 final). Brussels.
56. European Commission. (2009). Critical information infrastructure protection: "Protecting europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (No. COM(2009) 149).
57. ENISA. (2014). Technical guideline on security measures for Article 4 and Article 13a. Heraklion, Crete.
58. ENISA. (2015a). Information sharing in focus at ENISA's 3rd electronic communications reference group meeting.
59. ENISA. (2013). 1st meeting of ENISA's electronic communications reference group in Rome.
60. ENISA. (2012). Shortlisting network and information security standards and good practices. Heraklion, Crete.
61. ENISA. (2015b). Work programme 2016.
62. Council of the European Union. (2009). Council resolution of 18 December 2009 on a collaborative European approach to Network and Information Security (No. 2009/C 321/01). Brussels.
63. European Commission. (2010b). Europe 2020: A strategy for smart, sustainable and inclusive growth (No. COM(2010) 2020 final). Brussels.
64. Farrand, B. (2014). The digital agenda for Europe, the economy and its impact Upon the development of EU copyright policy, in: Stamatoudi, I.A., Torremans, P. (Eds.), Copyright law in the European union. Edward Elgar, Cheltenham.
65. European Commission. (2013a). Action 28: Reinforced Network and Information Security Policy [WWW Document]. Digital Agenda for Europe. URL ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-28-reinforced-network-and-information-security-policy (Accessed 12 June 2016).
66. European Commission, High Representative of the European Union for Foreign Affairs and Security Policy. (2013). Cybersecurity strategy of the European Union: An open, safe and secure cyberspace (No. JOIN(2013) 1). Brussels.

67. European Commission. (2013b). Commission staff working document: impact assessment accompanying the document: Proposal for a directive of the european parliament and of the council concerning measures to ensure a high level of network and information security across the union (No. SWD(2013) 31 final). Brussels.
68. European Commission. (2013c). Proposed directive on network and information security – frequently asked questions (No. IP/13/94). Brussels.
69. European Commission. (2015). EU cybersecurity strategy - 2nd High Level Conference [WWW Document]. Digital Agenda for Europe. URL ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-strategy-2nd-high-level-conference (Accessed 12 June 2016).
70. European Parliament. (2015). MEPs close deal with Council on first ever EU rules on cybersecurity [WWW Document]. European Parliament News. URL http://www.europarl.europa.eu/news/en/news-room/20151207IPR06449/MEPs-close-deal-with-Council-on-first-ever-EU-rules-on-cybersecurity (accessed 2.22.16).
71. Council of the European Union. (2016). 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 - political agreement (No. 5894/16).