Cybersecurity: towards a global standard in the protection of critical information infrastructures

Antonio Segura Serrano [1]

Cite as Segura Serrano A., "Cybersecurity: towards a global standard in the protection of critical information infrastructures", in European Journal of Law and Technology, Vol 6, No 3, 2015.

ABSTRACT

Protection of critical information infrastructures from cyber-attacks is becoming an acute problem for nation states. Cybersecurity has turned into a national policy priority while 'sovereignty considerations' appear to be increasingly important. National cybersecurity strategies seek to drive economic and social prosperity and protect cyberspace-reliant societies against cyber-threats. The US and the EU are among the first regulatory powers that have adopted important initiatives in the cybersecurity field. Moreover, cybersecurity is nowadays very high on the international agenda so that important efforts have also been undertaken by international fora like the G8, the United Nations, the OECD and the International Telecommunication Union (ITU). This paper argues that the adoption of clear, mandatory obligations regarding the setting up of information sharing and technology standards is the best normative option. This legal response is swiftly becoming the new global standard regarding the protection of critical information infrastructures. The approach based on voluntary standards and soft-law experienced in the US for the last twenty years has proved to be insufficient in order to provide a real improvement in this field. This is why, in order to cope with this policy problem, the latest proposal released by the US Administration is seeking to introduce a coherent public response based on more compulsory regulation. Likewise, the EU Network and Information Security (NIS) Directive Proposal has always pointed towards the establishment of a regulatory regime applicable to authorities and private operators alike. This emerging global standard was also to some extent suggested in the ITU National Cybersecurity Strategy Guide of 2012, which called for mandatory security standards.

Keywords: Cybersecurity; Critical information infrastructures; Information sharing; Executive Order 13,636; Cyber Intelligence Sharing and Protection Act (CISPA); Network and Information Security (NIS) Directive

1. A CHALLENGING LANDSCAPE

Protection of critical information infrastructures from cyber-attacks is becoming an acute problem for nation states. There are even predictions that extraordinary costs will probably be incurred in cybersecurity spending in order to avoid hacking effects. [2] The US Executive Order of 2013 adopted by Barack Obama [3] states that 'the cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront.' Similarly, the EU is aware of the digital world's vulnerability and has stated in its recent Cybersecurity Strategy that 'cybersecurity incidents, be it intentional or accidental, are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity or mobile services. Threats can have different origins - including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.' [4]

Cybersecurity policy making is at a turning point as a recent OECD report demonstrates. [5] Cybersecurity has become a national policy priority while 'sovereignty considerations' appear as increasingly important. National cybersecurity strategies seek to drive economic and social prosperity and protect cyberspace-reliant societies against cyber-threats. [6] Some common elements of these strategies are the enhancement of governmental co-ordination at policy and operational levels; the reinforcement of public-private cooperation; the emphasis on the need to respect fundamental values such as privacy, freedom of speech, and the free flow of information; and the call for improved international co-operation. [7] Finally, national cybersecurity strategies usually include an action plan for the protection of critical information infrastructures. [8]

This paper aims to elucidate how the US and the EU are among the first regulatory powers that have adopted important initiatives in the cybersecurity field. Moreover, cybersecurity is nowadays very high on the international agenda so that important efforts have also been undertaken by international fora like the G8, the UN, the OECD and the ITU. However, this paper argues that the different approach taken by the US and the EU regarding this domain is not tenable in the long run and is also counterproductive in order to achieve the main goal of improving cybersecurity. Most likely, future events will push national authorities, and at the international level as well, towards adopting a more regulatory stance than is the case now, giving way to a new global standard in this field.

2. THE INTERNATIONAL ARENA

The *G8 Principles for Protecting Critical Information Infrastructures* adopted in May 2003 was one of the first steps taken in this field at the international level. [9] This document offers a definition of effective critical infrastructure protection, which 'includes identifying threats to and reducing the vulnerability of such infrastructures to damage or attack, minimizing damage and recovery time in the event that damage or attack occurs, and identifying the cause of damage or the source of attack for analysis by experts and/or investigation by law enforcement'. [10] The G8 document puts forward eleven principles and encourages countries to consider them, including principles like having emergency warning networks,

raising awareness, promoting partnership among stakeholders both public and private, adopting legislative measures (with a mention of the Council of Europe Cybercrime Convention of 23 November 2001), and engaging in international cooperation.

The United Nations General Assembly has adopted several Resolutions regarding cybersecurity and the protection of critical information infrastructures. Resolution 58/199 and Resolution 64/211 are the most significant. [11] The former invites UN Member States and International Organizations to take into account some elements for protecting critical information infrastructure, endorsing almost literally the G8 Principles already mentioned. The latter goes further and offers a voluntary self-assessment tool for national efforts to protect critical information infrastructures.

After the 'Security Guidelines' in 2002, [12] now under revision, [13] the OECD adopted a specific initiative on the protection of critical information infrastructures, which are defined as 'those interconnected information systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy'. [14]Part I is devoted to the protection of critical information infrastructures at the domestic level and recommends member countries to demonstrate government leadership and commitment through the adoption of clear policy objectives and the setting up of government agencies with responsibility and authority to implement them. It also recommends the adoption of a national risk management strategy, including a risk management process setting out the detailed organization, tools and monitoring mechanisms required to implement the risk management strategy at every level, and the creation of a computer security incident response team (CERT/CSIRT). Finally, it recommends working in partnership with the private sector in order to enable 'mutual and regular exchange of information by establishing information sharing arrangements'. [15] Part II addresses the protection of critical information infrastructures across borders and promotes the engagement in bilateral and multilateral cooperation at regional and global levels with a view to sharing knowledge and experience, developing common understanding to facilitate collective action on vulnerabilities, and enabling robust information-sharing. [16]

The ITU was entrusted by the World Summit on the Information Society (WSIS) in 2005 to take the lead as the sole facilitator for Action Line C5, 'Building confidence and security in the use of information and communication technologies (ICTs)'. [17] In 2007, the ITU Secretary-General launched the Global Cybersecurity Agenda (GCA), subsequently endorsed by ITU Membership, which is a framework for international cooperation in cybersecurity, [18] and operationalized through the International Multilateral Partnership Against Cyber Threats (IMPACT). [19] IMPACT is labelled as 'the first comprehensive public-private partnership against cyber threats' and 'is tasked by ITU with the responsibility to provide ITU's 193 Member States access to expertise, facilities and resources to effectively address cyber threats, as well as assisting, as required, UN's agencies in protecting their ICT infrastructures'. [20] By the way, delivering support to developing countries in this field is an undertaking also carried by the World Bank. [21] The GCA is built upon five strategic pillars: the first three, i.e. legal framework, technical measures, and organizational structures need to be undertaken at the national and regional levels but also

harmonized at the international level. The last two pillars, i.e. capacity building and international cooperation, cross-cut in all areas. Moreover, the GCA is made up of seven main strategic goals. [22] On the basis of the GCA, the ITU produced a *National Cybersecurity Strategy Guide*. [23] This Guide includes a national cybersecurity strategy model that provides a holistic view of the cybersecurity domain (Figure 1).

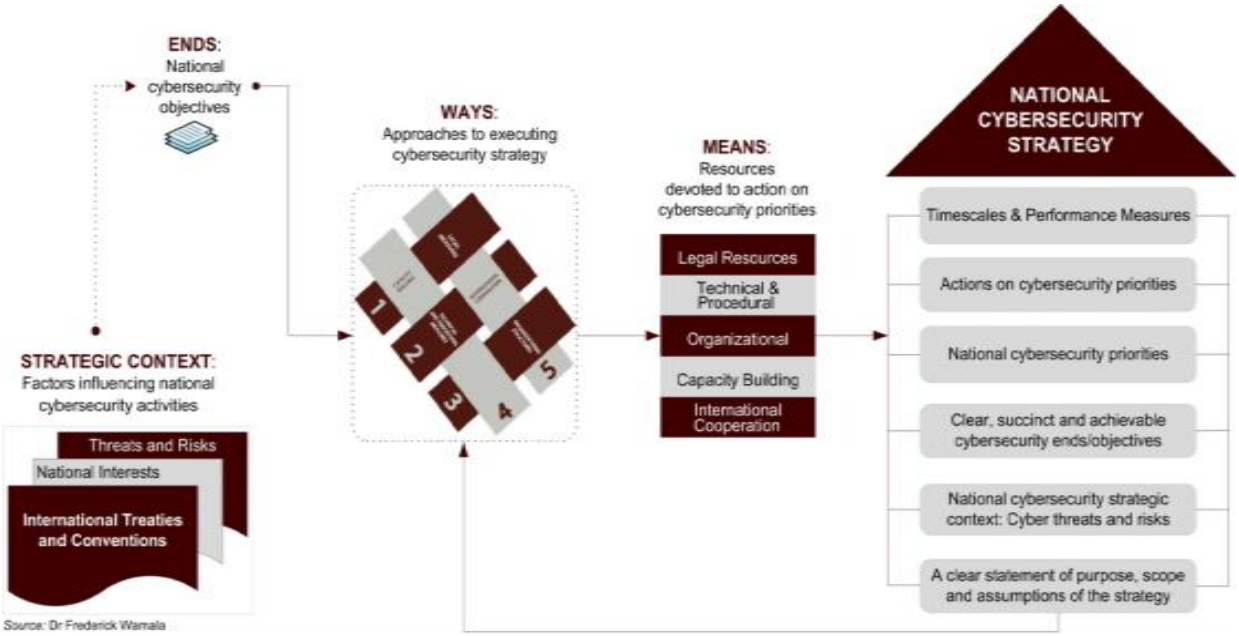

Figure 1 - Source: ITU National Cybersecurity Strategy Guide 2012

This model for national administrations seeking to elaborate new or improve existing National Strategies on Cybersecurity focuses on the strategic pillars that typically help a country create coherent national and globally compatible programs for protecting critical infrastructure against cyber threats. Apart from adopting legal measures, and among the technical/procedural measures to be taken, the Guide recommends the adoption of a 'National Cybersecurity Framework' (modelled on the ISO/IEC 27000 Series of standards) that defines mandatory security standards and offers guidance on issues such as risk management, compliance and assurance. [24] Among the organizational structures to be adopted, the Guide also recommends the creation of a National Cybersecurity Agency to coordinate efforts, a national Computer Incident Response Team (CIRT), and a Public-Private Partnership to enable real time exchange of information about cyber threats and vulnerabilities. [25]

3. THE UNITED STATES

Most probably, cybersecurity policy making at national level was first initiated by the US through Presidential Directive 63 adopted by President Clinton in 1998. [26] However, the US strategy regarding cybersecurity has been difficult to settle in the past as several bills tried to make their way in Congress unsuccessfully. [27] More recently, some proposed legislation like the Cyber Intelligence Sharing and Protection Act (CISPA) [28] and the SECURE IT Act, both supported by Republicans, as well as the Cybersecurity Act of 2012, [29] supported by Democrats, have followed suit and never passed, due in part to a harsh

criticism by civil rights activists and advocates of Internet privacy. [30] The latest proposal, the Cybersecurity Information Sharing Act (CISA), was introduced in the Senate in July 2014, and was passed on October 27, 2015. [31] The CISPA has been reintroduced again in January 2015. [32]

Therefore, the US strategy is currently based on an Executive Order adopted by President Obama on February 12, 2013, [33] together with a Presidential Policy Directive (PPD-21), [34] although new and more assertive measures have already been announced. [35] The Order offers a very large concept of 'critical infrastructure', which includes 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.' [36] Specifically, PPD-21 identifies sixteen critical infrastructure sectors, where internet service providers (ISPs) are included in both the communications sector and the information technology sector. [37] In order to improve security of the cyber critical infrastructure, the Order takes a holistic approach that is meant to address the three main areas of concern: information sharing, a risk-based Framework of core practices based on existing standards, and privacy protections. [38] Leaving aside the issue of privacy protection, both the information sharing and the Framework programs are the core tools used by this Order and both are voluntary, although that may change if Congress eventually adopts new legislation on the subject.

3.1 INFORMATION SHARING

It is considered a national priority to increase 'the volume, timeliness and quality of cyber threat information shared with authorized individuals and companies.' [39] The main goal of that Order is to enable information sharing between the private sector and all levels of government. [40] The Order promotes the fostering of public-private sharing in two ways. First, it directs the Secretary of Homeland Security and the Director of National Intelligence to establish a process for the timely notification to companies of information indicating that a company is the victim of a cyber-intrusion. In order to achieve this goal, the Order mandates the production and dissemination of both unclassified and classified reports of cyber threats to targeted entities. [41] The Order directs the Department of Homeland Security (DHS) to: [42]

Expedite the processing of clearances for appropriate state and local government and private sector personnel to enable the federal government to efficiently share cyber threat information at the sensitive and classified level.

Second, and perhaps more importantly, the Executive Order directs the Secretary of Homeland Security, together with the Secretary of Defence, to expand the Enhanced Cybersecurity Services (ECS) program to all critical infrastructure sectors, providing near real-time sharing of information on cyber threats to critical infrastructure companies and state and local governments. [43]

Most critical infrastructure entities already utilize cybersecurity providers to protect their networks. [44] The ECS is a voluntary program based on the sharing of indicators of

malicious cyber activity between DHS and participating ISPs. The ECS program interfaces with ISPs and offers an enhanced approach to protecting these entities by supplementing existing services and commercial capabilities with U.S. Government cyber threat information. This program serves to analyse information that is specific to identifying known or suspected cyber threats from a number of sources in the form of 'indicators'. [45] An indicator can be defined as human-readable cyber data used to identify some form of malicious cyber activity and are data related to IP addresses, domains, email headers, files, and strings. [46] These 'indicators' can be used to create intrusion detection signatures which are specific machine readable patterns of network traffic that are developed to identify and counter known or suspected cyber threats. Signatures are provided to firms or their ISPs to help counter known malicious cyber activity. [47] Through the use of signatures to counter threats, the ECS program introduces a whole new approach. It does not require human action to respond to reports. The ECS enables privately operated networks to take advantage of private government information in real time through an automated system that is able to stop an attack before it succeeds. [48] But, even if the statutory authority for ECS is granted as long as the program is voluntary, there remain constitutional constrains that might arise regarding information sharing. [49]

As regards the information sharing policy set up by the Executive Order, it is not a completely new initiative, as US agencies have been running information sharing pilot programs for some time, like the ECS program that the Order itself wants to expand, but also the Cyber Information Sharing and Collaboration Program (CISP) of 2011, [50] and the National Cybersecurity and Communications Integration Centre (NCCIC) of 2009.[51] This policy is considered an improvement over previously proposed legislation as it avoids serious privacy concerns by being privacy-neutral,[52] and apart from being merely 'voluntary', it focuses only on critical infrastructure, which means it will not hinder online commerce. [53]However, the information sharing plan proposed by the Executive Order is confronted with several criticisms, like the problem of mistrust derived from the Snowden's NSA leaks, the question of funding of this information-sharing policy, or the fear regarding the possibility that the voluntary character of those programs may become mandatory. [54] Moreover, it is submitted that the absence of any kind of empirical assessment between information sharing and the number and severity of cyber incidents makes this program ineffective, which in turn somehow justifies the reluctance of the private sector to participate. [55]

3.2 CYBERSECURITY FRAMEWORK

The Cybersecurity Framework seeks to establish risk-based cybersecurity standards as a result of a collaborative work with the industry. [56] The Executive Order mandates a leadership role for the National Institute of Standards and Technology (NIST) in developing a framework to reduce cyber risks to critical infrastructure. This Framework 'shall include a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.' [57] However, the Order mandates the Framework to 'incorporate voluntary consensus standards and industry best practices to the fullest extent possible', including 'voluntary international standards'. [58] Accordingly,

existing voluntary consensus standards and best practices from the private sector would be ascertained by NIST, and incorporated into the framework. [59]

The Cybersecurity Framework was also drafted to provide a 'prioritized, flexible, repeatable, performance-based, and cost-effective approach' to help technology service operators 'identify, assess, and manage' risks, and focusing on determining 'cross-sector security standards and guidelines applicable to critical infrastructure.' The Cybersecurity Framework would facilitate guidance about neutral technologies, enabling 'critical infrastructure sectors to benefit from a competitive market for products and services'. [60] In so doing, the US Administration made clear that this framework did not imposed a unified solution to all cases. On the contrary, it encourages a cooperative approach to boost innovation and recognize that critical infrastructure sectors have different needs. Entities that wish to improve their cybersecurity will have the possibility to obtain from the market a variety of state of the art products and services. [61]

The NIST released on February 2014 the voluntary risk based Cybersecurity Framework as a set of industry standards and best practices to help organizations manage cybersecurity risks, as the result of a collaborative process between government and the private sector. The Framework promotes the use of business drivers to outline cybersecurity activities and regards cybersecurity risks as a question of every entity's risk management. The Framework is made up of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers.[62]

The Framework Core is a set of common cybersecurity activities and desired outcomes, and consists of five simultaneous and continuous functions, i.e., identify, protect, detect, respond, and recover. After evaluation, these functions provide a sophisticated, strategic view of an entity's management of cybersecurity risk. The Framework Implementation Tiers assess the extent to which an entity's cybersecurity risk management practices display the features defined in the Framework (e.g., risk and threat aware, repeatable, and adaptive). The Tiers allow an array of different entity practices to be depicted, from Partial (Tier 1) to Adaptive (Tier 4). The Framework Profile represents the alignment of standards, guidelines, and practices to the Framework Core by a given organization in a specific implementation setting. The aim is improving a cybersecurity stance from a current profile to a target profile. [63]

Regarding the Cybersecurity Framework, it was initially praised because it contains flexible standards which are not imposed as mandatory, but are the result of a collaborative engagement with the private sector, and reflect well settled industry security practices. [64] Even recently, the Framework has been assessed as a good starting point for trying to communicate the obscure subject of cybersecurity to managers, regulators, and vendors. [65]

Nevertheless, many commentators are critical regarding this Cybersecurity Framework. It is submitted that the Framework is unnecessary as 'many organizations have essentially 'adopted' the Framework elements long before the Framework, itself, was constructed'. [66] Moreover, the Framework has generated much misperception among private companies, which are left wondering about whether they have complied with their

duties. [67] At the same time, companies are nowadays worried about the perils of the Framework becoming mandatory through liability. [68] Last but not least, it is submitted that using the Framework will not assure critical infrastructure security: much more is needed and a misunderstanding in this field could lead to misguided public policies and also stall advancement and innovation. [69] To sum up, the Framework has been praised because it is flexible and voluntary, as opposed to including outright mandatory provisions. But the effort to delineate a program which is acceptable to private companies might be counterproductive for an actual improvement in cybersecurity. [70]

4. THE EUROPEAN UNION

The European policy devoted to strengthen the security of and the trust in the information society started with a Commission proposal in 2001, [71]and a strategy published in 2006. [72] However, as implementation by stakeholders appeared insufficient, in 2009 the EU Commission adopted a Communication squarely on critical information infrastructure protection. [73] Under and in parallel to the European Program for Critical Infrastructure Protection (EPCIP), [74] which sets out the global approach to the protection of critical infrastructures in the EU, the 2009 Communication focuses on the protection of Europe from cyber disruptions by enhancing security and resilience and defines information and communication technologies (ICT) infrastructures as those that 'form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as critical information infrastructures as their disruption or destruction would have a serious impact on vital societal functions'. [75] This Communication sets out an action plan, involving Member States and the private sector, which is based on five pillars: preparedness and prevention; detection and response (based on a European Information Sharing and Alert System); mitigation and recovery; international cooperation; and criteria for European Critical Infrastructures in the ICT sector. [76] In 2011, the Commission reviewed the results achieved until that moment and announced follow-up actions in a Communication, [77] which was endorsed by the Council of the European Union [78] and the European Parliament. [79]

Nevertheless, the EU took a major step in 2013 through a new Cybersecurity Strategy [80] that outlines the EU's vision in this domain, clarifies roles and responsibilities and sets out the actions required in this field. This strategy was launched together with a proposal for a Directive on Network and Information Security (NIS), [81] still under negotiation among the European institutions.

4.1 CYBERSECURITY STRATEGY

The 2013 Strategy spells out the principles that should guide cybersecurity policy both within the EU and in the international field. In this vein, the EU stresses that EU's core values apply as much in the digital as in the physical world, including the protection of fundamental rights, freedom of expression, personal data and privacy, and access for all. The EU vision presented in this Strategy is articulated in five strategic priorities, and proposes specific actions that can enhance the EU's overall performance. The first priority

consists of achieving cyber resilience. The Strategy states that 'Europe will remain vulnerable without a substantial effort to enhance public and private capacities, resources and processes to prevent, detect and handle cyber security incidents'. [82]

Together with the policy on NIS that will be evaluated below, the EU has already taken some steps in this direction, like the establishment of the European Network and Information Security Agency (ENISA) in 2004, [83] which supports Member States in developing robust 'national cyber resilience capabilities, notably by building expertise on security and resilience of industrial control systems, transport and energy infrastructure.'[84] Besides, the Digital Agenda for Europe (DAE) [85] adopted in 2010 stressed that trust and security are vital prerequisites for the extensive application of ICT, emphasizing the need for all stakeholders to cooperate in an all-inclusive effort to ensure the security and resilience of ICT infrastructure. In order to improve cyber resilience, the Strategy also purports to raise awareness *vis-a-vis* end users mainly through publishing reports, organizing expert workshops and developing public-private partnerships.

The second priority of the Strategy consists of drastically reducing cybercrime through strong and effective legislation (EU and internationally) and enhancing operational capabilities to combat it, including strengthening coordination at EU level. The third priority is to develop cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP), where the EU will aim at a cooperative effort between the EU and NATO to increase 'the resilience of critical governmental, defence and other information infrastructures.' [86] The fourth priority is to develop the industrial and technological resources for cybersecurity, by way of promoting a Single Market for cybersecurity products and fostering research and development investments and innovation. Finally, it is also a priority to establish a consistent international cyber policy for the EU and promote its core values through dialogue with third countries, with a special focus on like-minded partners. [87]

Regarding the classification of roles and responsibilities, the Strategy indicates that cybersecurity activities should span across three key pillars, i.e. NIS, law enforcement, and defence, which also operate within different legal frameworks (EU or national) and therefore involving several bodies at EU and Member State level. [88]

4.2 NETWORK AND INFORMATION SECURITY (NIS)

The Proposal for a Directive on NIS is the main action of the Strategy. It seeks to improve the security of the Internet and information systems, including private networks, which underpin the functioning of modern societies. [89] This aim will be achieved by imposing requirements on both Member States and operators of critical infrastructures such as energy, transport, and key providers of information society services (e-commerce platforms, social networks, etc.). The former will have to increase their preparedness and improve their cooperation. The latter will have to adopt appropriate steps to oversee security threats and report serious cases to the qualified national authorities. The Proposal highlights the current situation in the EU, which reflects a purely voluntary approach that is not effective protection against NIS incidents and risks across the EU.

In particular, with the exception of telecommunication companies, the players managing critical infrastructure or providing essential services (banking, stock exchanges, energy generation, transmission and distribution, transport, health, internet services and public administrations) are not under proper obligations to 1) adopt risk management measures, and 2) exchange information with relevant authorities. Therefore, a major change is needed in the way NIS is dealt within the EU and the Proposal envisages laying down regulatory obligations in order to create a level playing field and close existing legislative loopholes. [90]

The existing EU regulatory context is made up of several provisions. Providers of electronic communications are required by the Framework Directive to adequately manage their networks taking into account risks, and to notify significant security breaches. [91] Furthermore, EU Directives require data controllers to ensure compliance with requirements and safeguards, including security measures, in the field of data protection. In addition, in the sector of e-communication services, EU regulation obliges data controllers to report incidents involving a breach of personal data to the authorities in EU member countries. [92] Moreover, according to the General Data Protection Regulation proposed by the Commission in 2012,[93] data controllers would have to report breaches of personal data to Member State authorities. Under this new Regulation, a NIS security breach would not have to be notified if it occurs while a service is being provided but personal data is not affected, for instance as a result of a blackout. Also, under Directive 2008/114, [94] EPCIP sets out several goals fully consistent with the proposed NIS Directive. But EPCIP does not require operators to report significant security breaches and does not set up tools for the Member States to cooperate and react to incidents. Finally, there is a recent Directive on attacks against information systems [95] which harmonizes the criminalization of certain types of conduct, but it does not address NIS risks and incidents from the point of view of prevention, response, and mitigation of their impact.

The relevant operative provisions of the Directive Proposal concern the setting up of national frameworks on NIS, the creation of a cooperation network among national authorities and the Commission, and the establishment of security requirements *vis-a-vis* market operators. Firstly, Article 5 calls for each member nation to implement a national NIS strategy that will set out the strategic objectives and a defined scheme to preserve network security. Moreover, each Member State will designate a national 'competent authority' and a 'single point of contact' [96] on the security of network and information systems (Article 6) and will set up a Computer Emergency Response Team (CERT) (Article 7).

Second, the cooperation network made up of national authorities, the Commission and ENISA will cooperate against risks and incidents affecting network and information systems (Article 8) through a secure information-sharing system (Article 9). Article 10 provides for the possibility of early warnings within the cooperation network on those risks and incidents that may grow rapidly in scale, may exceed the capacity to respond at the national level, or may involve more than one nation. In case of early warning, the competent authorities are to agree on a coordinated response in accordance with the Union NIS cooperation plan referred to in Article 12.

Thirdly, Chapter IV of the Proposal contains the most important provisions which refer to security requirements and incident notification. Article 14 (1) provides that 'Member States shall ensure that […] market operators take appropriate technical and organizational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations'. Those measures have to be in line with the state of the art and ensure the continuity of the service. Moreover, the competent authority in Member States will be notified by market operators in case of incidents 'having a significant impact' on the security of the main services they provide (Article 14 (2)). The European Parliament has revised the proposed Directive and has offered several parameters in order to determine the 'significance of the impact', specifically the number of users whose core services is affected; the duration of the incident; and the geographic spread with regard to the area affected by the incident. [97] In case the incident is in the public interest, the public should also be informed (Article 14 (4)). Regarding incident notification, there is still an important disagreement between, on the one hand, Member States that prefer voluntary notification and argue that trust cannot be imposed and, on the other hand, those that believe that the Directive should result in firm commitments. [98] Article 15 deals with implementation and enforcement, and provides that competent authorities will have all the powers to investigate cases of non-compliance, to require market operators to provide information (including a third-party security audit), and to issue binding instructions to them. Article 17 (Chapter V) provides that Member States will lay down rules on sanctions (that must be 'effective, proportionate and dissuasive') applicable to infringements, and will take measures to ensure that they are implemented.

One of the most critical questions regarding the Proposal is the scope of 'market operator' (Article 3 (8)). According to this provision, market operator means: '(a) provider of information society services which enable the provision of other information society services; [99] (b) operator of critical infrastructure that are essential for the maintenance of vital economic and societal activities in the fields of energy, transport, banking, stock exchanges and health'. [100] However, there is still no agreement on whether or not to include in Annex II the identification of specific sectors, for example, information society services, banking and financial market infrastructures. [101] There is much criticism from experts in this respect. It is said that while the U.S. is focusing mostly on critical infrastructure operators (i.e., those operating in any of the sixteen sectors identified in PPD-21), the EU Commission Proposal is including key internet companies or 'information service providers', by way of example, search engines like Google and cloud providers like Apple. This approach may lead to increased administrative burdens for affected companies that must also comply with any new U.S. and EU cybersecurity requirements, [102] or may even provoke inconsistencies. [103] It is submitted that the Directive was successfully passed in the European Parliament in March 2014 thanks to the exemption of the 'internet enablers' from the list, [104] although the European Parliament widened the scope of the revised Directive to include the so-called Internet Exchange Points. However, a growing number of Member States are pushing for the inclusion of information society services at large, like cloud computing, application stores, search engines and social networks within the scope of the Directive. According to some, this would create 'a burdensome regulatory regime with no corresponding security benefit, it would also heighten the workload for often struggling regulatory agencies, and it would expose citizens' personal data to unnecessary

risk' [105] and, therefore, the European Union should limit itself to 'cyber attacks against truly critical infrastructures which could lead to catastrophic impacts on public safety, national security and the broader economy'. [106] According to others, 'the exclusion of Internet enablers could significantly water down the effect of the Directive.' [107] Be that as it may, the EU seems to have decided about the need to take a more regulatory approach than the US.

5. TOWARDS A GLOBAL STANDARD

International organizations and fora like the G8, the UN, the OECD, and the ITU have adopted meaningful initiatives to foster cybersecurity and protect critical information infrastructures. They are in the form of recommendations to States. Apart from the adoption of legislative measures, their common elements point to the setting up of national cybersecurity frameworks, cybersecurity agencies or coordinators, computer emergency response teams, and public-private partnerships (taking into account that most information networks are private). These initiatives indicate that international organizations currently rely on States to adopt measures that protect critical information infrastructures, according to a reference model. In other words, with the exception of the Council of Europe Cybercrime Convention, truly international action in cybersecurity policymaking seems unlikely in the near future, as States are eager to adopt assertive measures regarding Internet governance in the first place.[108]

The US and the EU have taken important steps in order to protect critical information infrastructures. The US 2013 Executive Order is not a legislative measure, but surely sets the stage regarding the approach that this country will uphold in the near future. Both the information sharing and the Cybersecurity Framework programs are the core tools used by this Order and both are voluntary. There are no mandatory obligations imposed on critical information operators, which are mostly private. Moreover, the US Executive Order is directed only to core critical information infrastructure operators comprised in any of the sixteen sectors identified by PPD-21, including ISPs. On the other hand, the information sharing program is meant to be unidirectional, from Government towards private entities, but not from private organisations towards Government. The logic of this approach is that cybersecurity activities should not affect legal protections like those regarding privacy. Therefore, the US has opted for adopting a strategy based on voluntary standards, which in turn can be labelled as a form of soft-law. In this way, the US hopes to set a standard that can be readily transposed abroad in order to build a global standard on critical information infrastructure protection, [109] while promoting the activities of US giants in the information society service sector.

However, as has been noted, there are several caveats to the voluntary approach. The 'purely voluntary approach to either cyber threat information sharing or technology adoption could hinder the effectiveness' of the Order and the Cybersecurity Framework and lead to inconsistent implementation. [110] Indeed, after conducting a cost-benefit analysis, private companies will neither be inclined to disclose the intrusions they have experienced nor reveal the vulnerabilities they have discovered. [111] This is the reason why the latest legislative proposals, e. g. CISPA and the 2015 White House Legislative Proposal, are

pointing towards a more regulatory approach in this field, while addressing privacy and other legal issues. [112] It is submitted that, if mandatory information sharing is finally adopted, anonymizing and aggregating disclosure information [113]within a sort of nongovernmental non-profit clearing house organization [114] should help to alleviate privacy- and antitrust-related concerns. Moreover, clearly stated liability protection would be needed in order to overcome the initial reluctance on the part of private entities.

By contrast, the EU policy regarding cybersecurity has adopted a different approach since its inception. The 2013 draft Directive under discussion seems to be inclined towards a clear regulatory approach where mandatory obligations will be imposed on public/private operators. Similarly, the scope of the Directive might eventually be wide enough so as to reach, not only core critical infrastructure operators, but most Internet services enablers. We are now precisely witnessing a battle between policy approaches in the EU regarding this issue. On the one hand, the European Parliament and some Member States like the UK are willing to include only core critical sectors considered essential, i.e., companies in the energy, transport, banking and health sectors. [115] On the other hand, the EU Commission and some Member States like Germany, France, and Spain want to include not only those already mentioned but also internet enablers, which may include e-commerce platforms, internet payment gateways, social networks, search engines, cloud computing services, and application stores. [116] The end result of the negotiating process will probably be closer to the latter approach and for good reasons. The rationale is that information society services may underpin some critical infrastructure, and without which market operators may not be able to operate. It is true that current negotiations within EU institutions are leading to a 'different treatment' of information society services. [117] However, the final result will be positive. This will mean that information sharing will be bidirectional (from Government towards private entities and from private entities towards Government) and that the Internet giants would be involved in the goal of achieving critical infrastructure protection. Search engines like Google and providers of cloud services like Apple could hugely help in the process of notifying major NIS incidents to the national and EU authorities which in turn may report to the critical infrastructure sectors affected, or even the public at large, in order to preserve the functioning and reliability of those systems. In this way, the EU approach has the potential to set an example to the rest of the world regarding the interests and values to be preserved through legislation in this field. [118]

This paper argues that the adoption of clearly mandatory obligations regarding the setting up of information sharing and technology standards is the best normative option. This legal response is swiftly becoming the new global standard regarding the protection of critical information infrastructures. The approach based on voluntary standards and soft-law experienced in the US for the last twenty years has proved to be insufficient in order to provide a real improvement in this field. This is why, in order to cope with this policy problem, the latest proposal released by the US Administration is seeking to introduce a coherent public response based on more compulsory regulation. Likewise, the EU NIS Directive Proposal has always pointed towards the establishment of a regulatory regime applicable to authorities and private operators alike (including Internet service giants like Google, Facebook and Apple). This emerging global standard was to some extent suggested in the ITU National Cybersecurity Strategy Guide already analysed, which called for

mandatory security standards. But of course, more efforts will be needed at the international level to effectively implement cooperation among States sharing this regulatory approach.

6. CONCLUDING REMARKS

The divergences found between the US and the EU approaches are just negligible if we compare them with the approaches of other countries like China, where cybersecurity is an open concept that may also include the ability to control the content available on the Web. Even if the warnings about a new 'digital divide' [119] are overstated, the process of arriving at a common ground in this field will surely be a challenging task. When reciprocal trust is lacking, [120] the prospect of multilateral efforts towards the development of shared international standards or best practices, not to mention global regulatory norms, seems unlikely in the near future. Unfortunately, the result of this process might be more, instead of fewer, conflicting legal regimes. [121]

Alternatively, it would be wise to adopt a more regulatory approach in order to set up mandatory obligations that would apply to public and private entities involved in the critical information infrastructure domain. The US itself is moving ahead towards adopting more mandatory obligations in this field. The CISPA and the 2015 Legislative Proposal both point in this direction. Similarly, the EU NIS Directive Proposal will most probably include compulsory obligations with respect to information sharing as well as technical and organizational measures for virtually all market operators to manage the risks posed to the systems that they control.

Instead of a soft-law global standard, the regulatory approach which is already developing within the US and the EU will likely be transposed onto the international plane and will spur other initiatives, whether in the ITU or other international organizations, in order to mandate information sharing obligations whenever a threat to critical information infrastructure is at stake. Of course, national interests and sovereign issues regarding defensive and offensive cybersecurity capabilities always emerge once we reach the global arena and may cause States to refrain from adopting a purely cooperative approach. However, as soon as it becomes clear that the gains outweigh the costs, the regulatory approach will also be transformed into a cooperative strategy in the international context, through the adoption of an international treaty or otherwise. We are now witnessing the emergence of this new global standard and it will surely take some time before we see practical results from this change in the approach, but there seems to be no other way forward.

---

[1] Associate Professor, Department of Public International Law and International Relations, University of Granada.

[2] ABI Research, '$US100 Billion Cybersecurity Spending for Critical Infrastructure by 2020', *Analyst Insider*, October 29, 2014, accessed October 29,

2014, https://www.abiresearch.com/market-research/service/cybersecurity-strategies-for-critical-infrastructure/ .

[3] Executive Order (EO) 13,636, 'Improving Critical Infrastructure Cybersecurity', February 12, 2013, Sec. 1, accessed June 27, 2014,http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity .

[4] European Commission, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 'Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace', JOIN (2013) 1 final, 7.2.2013, 3.

[5] OECD, 'Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy', 2012.

[6] OECD, 2012, 9.

[7] OECD, 2012, 13-14.

[8] Other key priority areas are government security, the fight against cybercrime, awareness raising, education and response (in terms of a Cyber Security Incident Response Team), OECD, 2012, 16.

[9] G8 Principles for Protecting Critical Information Infrastructures (adopted by the G8 Justice & Interior Ministers, May 2003), accessed June 16, 2014, http://www.infrastrutturecritiche.it/aiic/index.php?option=com_docman&task=doc_download&gid=111&Itemid=99 .

[10] G8 Principles for Protecting Critical Information Infrastructures, 2014.

[11] United Nations General Assembly Resolution 58/199, 'Creation of a global culture of cybersecurity and the protection of critical information infrastructures', A/RES/58/199, January 30, 2004; United Nations General Assembly Resolution 64/221 'Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures', A/RES/64/221, March 17, 2010.

[12] OECD, 'Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security' [C(2002)131], July 25, 2002.

[13] OECD, 'OCDE Reviewing Its Security of Information Systems and Networks Guidelines', April 8, 2013, accessed June 17, 2014,https://ccdcoe.org/oecd-reviewing-its-security-information-systems-and-networks-guidelines.html .

[14] OECD, 'Recommendation of the Council on the Protection of Critical Information Infrastructures' [C(2008)35], April 30, 2008, 4.

[15] OECD Recommendation, 2008, 5-6.

[16] OECD Recommendation, 2008, 6-7.

[17] World Summit on the Information Society, Geneva 2003-Tunis 2005, 'Tunis Agenda for the information society', WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 November 2005, accessed June 16, 2014, http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf.

[18] ITU, 'Global Cybersecurity Agenda', 2007, accessed June 16, 2014, http://www.intgovforum.org/Substantive_2nd_IGF/ITU_GCA_E.pdf.

[19] IMPACT, accessed June 17, 2014, http://www.impact-alliance.org/home/index.html.

[20] IMPACT, 'Mission and Vision', accessed June 17, 2014, http://www.impact-alliance.org/aboutus/mission-&-vision.html.

[21] The World Bank Group, 'ICT for Greater Development Impact - World Bank Group Strategy for Information and Communication Technology 2012-2015', June 15, 2012, accessed June 16, 2014,http://siteresources.worldbank.org/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/Resources/WBG_ICT_Strategy-2012.pdf .

[22] ITU, 'Global Cybersecurity Agenda', 15.

[23] ITU, 'National Cybersecurity Strategy Guide', 2012, accessed June 16, 2014, http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf .

[24] ITU, 'National Cybersecurity Strategy Guide', 2012, 75.

[25] ITU, 'National Cybersecurity Strategy Guide', 2012, 60-67.

[26] Presidential Decision Directive (PDD)-63, 'Critical Infrastructure Protection', May 22, 1998, accessed June 16, 2014,http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[27] Cyber Security Information Act, H.R. 2435 - 107th Cong. (1st Sess. 2001); Cyber Security Enhancement Act of 2002, H.R. 3482 - 107th Cong. (2d Sess. 2002); Cyber Security Information Act of 2000, H.R. 4246 - 106th Cong. (2d Sess. 1999).

[28] Cyber Intelligence Sharing and Protection Act, H.R.3523 - 112th Congress (2011-2012); reintroduced in 2013, H.R.624 - 113th Congress (2013-2014).

[29] Cybersecurity Act of 2012, S. 2105, 112th Congress (2d Sess. 2012).

[30] Mark Jaycox and Kurt Opsahl, 'CISPA is Back: FAQ on What it is and Why it's Still Dangerous', *Electronic Frontier Foundation*, February 25, 2013, accessed June 16, 2014, https://www.eff.org/cybersecurity-bill-faq.

[31] Cybersecurity Information Sharing Act, S.754 - 114th Congress (2015-2016). Mark Jaycox, 'A Zombie Bill Comes Back to Life: A Look at The Senate's Cybersecurity Information Sharing Act of 2014', *Electronic Frontier Foundation*, June 29, 2014, accessed

September 15, 2014,https://www.eff.org/deeplinks/2014/06/zombie-bill-comes-back-look-senates-cybersecurity-information-sharing-act-2014 .

[32] Cyber Intelligence Sharing and Protection Act, H.R.234 - 114th Congress (2015-2016). Kate Knibbs, 'The New CISPA Bill Is Literally Exactly the Same as the Last One', *Gizmodo*, January 14, 2015, accessed November 9, 2015, http://gizmodo.com/the-new-cispa-bill-is-literally-exactly-the-same-as-the-1679496808 .

[33] Exec. Order No. 13,636.

[34] Presidential Policy Directive (PPD)-21, 'Critical Infrastructure Security and Resilience', February 12, 2013, accessed June 27, 2014,http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil .

[35] The White House, Office of the Press Secretary, 'Securing Cyberspace - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts', January 13, 2015, accessed January 16, 2015, http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat . Mark Jaycox and Lee Tien, 'EFF Statement on President Obama's Cybersecurity Legislative Proposal', *Electronic Frontier Foundation*, January 13, 2015, accessed January 16, 2015, https://www.eff.org/deeplinks/2015/01/eff-statement-president-obamas-cybersecurity-legislative-proposal .

[36] Exec. Order No. 13,636, Sec. 2.

[37] PPD-21 identifies the following sixteen critical infrastructure sectors: Chemical, Commercial Facilities, Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Financial Services, Food and Agriculture, Government Facilities, Healthcare and Public Health, Information Technology, Nuclear Reactors, Materials, and Waste, Transportation Systems, and Water and Wastewater Systems.

[38] Michael Daniel, Special Ass't to the President and White House Cybersecurity Coordinator, 'Improving the Security of the Nation's Critical Infrastructure', *The White House Blog*, February 13, 2013, 6:39
PM, http://www.whitehouse.gov/blog/2013/02/13/improving-security-nation-s-critical-infrastructure .

[39] Michael Daniel, 'Improving the Security of the Nation's Critical Infrastructure'.

[40] Michael Daniel, 'Improving the Security of the Nation's Critical Infrastructure'.

[41] Exec. Order No. 13,636, Sec. 4 (a) (unclassified reports), Sec. 4 (b) (classified reports).

[42] Exec. Order No. 13,636, Sec. 4 (d).

[43] Exec. Order No. 13,636, Sec. 4 (c). See also Improving the Security of the Nation's Critical Infrastructure,http://www.whitehouse.gov/blog/2013/02/13/improving-security-nation-s-critical-infrastructure .

[44] U. S. Department of Homeland Security, 'Enhanced Cybersecurity Services', September 8, 2014, accessed June 16, 2014,http://www.dhs.gov/enhanced-cybersecurity-services.

[45] U. S. Department of Homeland Security, 'Privacy Impact Assessment for the Enhanced Cybersecurity Services (ECS)', DHS/NPPD/PIA-028, January 16, 2013, 3, accessed June 16, 2014, http://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_nppd_ecs_jan2013.pdf .

[46] U. S. Department of Homeland Security, 'Privacy Impact Assessment for the Enhanced Cybersecurity Services (ECS)', 2, footnote 2.

[47] Michael Daniel, '007 or DDoS: What is Real World Cyber?', February 28, 2013: 3, accessed June 16, 2014,http://www.whitehouse.gov/sites/default/files/docs/2013-02-28_final_rsa_speech.pdf .

[48] Jeremi G. Broggi, 'Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes', *Harvard Journal of Law & Public Policy* 37 (2014): 658.

[49] Jeremi G. Broggi, 'Building on Executive Order 13,636 to Encourage Information Sharing for Cybersecurity Purposes', 658-60.

[50] Department of Homeland Security, 'CIKR Cyber Information Sharing and Collaboration Program (CISCP)', June 2013, accessed September 15, 2014, http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_menna_ciscp_one_pager.pdf .

[51] Department of Homeland Security, 'Secretary Napolitano Opens New National Cybersecurity and Communications Integration Centre', October 30, 2009, accessed September 15, 2014, http://www.dhs.gov/news/2009/10/30/new-national-cybersecurity-center-opened .

[52] Michelle Richardson, 'President Obama Shows No CISPA-like Invasion of Privacy Needed to Defend Critical Infrastructure', *ACLU*, February 13, 2013, accessed September 15, 2014, https://www.aclu.org/blog/national-security-technology-and-liberty/president-obama-shows-no-cispa-invasion-privacy-needed .

[53] Robert Gyenes, 'A Voluntary Cybersecurity Framework Is Unworkable - Government Must Crack the Whip', *Pittsburgh Journal of Technology Law & Policy* 14 (2014): 301.

[54] Robert Gyenes, 'A Voluntary Cybersecurity Framework Is Unworkable', 304.

[55] Matthew H. Fleming, Eric Goldstein, and John Roman, 'Evaluating the Impact of Cybersecurity Information Sharing on Cyber Incidents and Their Consequences', January 17, 2014, 4, accessed September 15, 2014, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418357.

[56] Mélanie J. Teplinsky, 'Fiddling on the Roof: Recent Developments in Cybersecurity', *American University Business Law Review* 2 (2013): 300.

[57] Exec. Order No. 13,636, Sec. 7 (a).

[58] Exec. Order No. 13,636, Sec. 7 (a).

[59] Michael Daniel, 'Improving the Security of the Nation's Critical Infrastructure', 2.

[60] Exec. Order No. 13,636, Sec. 7 (b).

[61] Michael Daniel, 'Improving the Security of the Nation's Critical Infrastructure', 2.

[62] National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity', Version 1.0, February 12, 2014, accessed June 16, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf .

[63] National Institute of Standards and Technology, 'Framework for Improving Critical Infrastructure Cybersecurity', 4-5.

[64] Cynthia Brumfield, 'NIST framework released to widespread praise, but what happens next?', *CSO Online*, February 13, 2014, accessed September 15, 2014, http://www.csoonline.com/article/2134401/metrics-budgets/nist-framework-released-to-widespread-praise--but-what-happens-next-.html .

[65] Cynthia Brumfield, 'Four Key Take-Aways from the Sixth NIST Cybersecurity Framework Workshop', *DigitalCrazyTown*, November 6, 2014, accessed December 1, 2014, http://www.digitalcrazytown.com/2014/11/four-key-take-aways-from-sixth-nist.html .

[66] Internet Security Alliance, 'Executive Summary Assessing President Obama's Executive Order on Cyber Security', February 6, 2014, 5, accessed September 15, 2014, http://isalliance.org/publications/Assessing%20Executive%20Order%20Success%20-%20ISA%20Criteria%20Paper%20-%20Final%202-6-14.pdf .

[67] Joab Jackson, 'How the NIST cybersecurity framework can help secure the enterprise', *PCWorld*, February 14, 2014, accessed September 15, 2014,http://www.pcworld.com/article/2098320/how-the-nist-cybersecurity-framework-can-help-secure-the-enterprise.html .

[68] Jason Wool, 'Takeaways From NIST Workshop on Cybersecurity Framework', *Law 360*, November 7, 2014, accessed December 2, 2014,http://www.law360.com/articles/594633/takeaways-from-nist-workshop-on-cybersecurity-framework .

[69] Internet Security Alliance, 'Executive Summary Assessing President Obama's Executive Order on Cyber Security', 4.

[70] Robert Gyenes, 'A Voluntary Cybersecurity Framework Is Unworkable', 307.

[71] European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 'Network and Information Security: Proposal for a European Policy Approach', COM (2001) 298 final, 6.6.2001.

[72] European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions, 'A strategy for a Secure Information Society - Dialogue, partnership and empowerment', COM (2006) 251 final, 31.5.2006.

[73] European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection - 'Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience', COM (2009) 149 final, 30.3.2009.

[74] European Commission, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM (2006) 786 final, 12.12.2006.

[75] COM (2009) 149 final, 2.

[76] COM (2009) 149 final, 8.

[77] European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber-security', COM (2011) 163 final, 31.3.2011.

[78] Council of the European Union, 'Conclusions' (10299/11), 19 May 2011, accessed June 16,
2014, http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010299%202011%20INIT .

[79] European Parliament, 'Resolution of 12 June 2012 on critical information infrastructure protection - achievements and next steps: towards global cyber-security', (P7_TA(2012)0237), accessed June 16,
2014, http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2012-0237&language=EN&ring=A7-2012-0167 .

[80] JOIN (2013) 1 final.

[81] European Commission, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM (2013) 48 final, 7.2.2013.

[82] JOIN (2013) 1 final, 5.

[83] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, *O.J.* L

77/1, 13.3.2004. Regulation (EC) 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, *O.J.* L 165/41, 18.6.2013.

[84] JOIN (2013) 1 final, 7.

[85] European Commission, Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions 'A Digital Agenda for Europe', COM (2010) 245 final, 19.5.2010.

[86] JOIN (2013) 1 final, 11.

[87] JOIN (2013) 1 final, 12-16.

[88] JOIN (2013) 1 final, 17.

[89] COM (2013) 48 final, 2.

[90] COM (2013) 48 final, 4.

[91] Article 13 (a) & (b) of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive), *O.J.* L 108/33, 24.4.2002. Amended by Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, *O.J.* L 337/37, 18.12.2009.

[92] Article 17 of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *O.J.* L 281 /31, 23.11.95. Article 4 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), *O.J.* L 201/37, 31.7.2002.

[93] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final, 25.1.2012.

[94] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, *O.J.* L 345/75, 23.12.2008.

[95] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, O.J. L 218/8, 14.8.2013.

[96] Council of the European Union, 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 - Preparations for the 1st informal exploratory trilogue, Doc. 13848/14, October 13, 2014, 22.

[97] European Parliament, Report on the 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, A7-0103/2014, 12.2.2014, 53.

[98] Council of the European Union, Doc. 13848/14, 3.

[99] Annex II sets out a non-exhaustive list: e-commerce platforms, Internet payment gateways, social networks, search engines, cloud computing services, application stores, COM (2013) 48 final, 30.

[100] Annex II sets out a non-exhaustive list: 1. Energy: electricity and gas suppliers, electricity and/or gas distribution system operators and retailers for final consumers, natural gas transmission system operators, storage operators and LNG operators, transmission system operators in electricity, oil transmission pipelines and oil storage, electricity and gas market operators, operators of oil and natural gas production, refining and treatment facilities; 2. Transport: air carriers (freight and passenger air transport), maritime carriers (sea and coastal passenger water transport companies and sea and coastal freight water transport companies), railways (infrastructure managers, integrated companies and railway transport operators), airports, ports, traffic management control operators, auxiliary logistics services (warehousing and storage, cargo handling and other transportation support activities); 3. Banking: credit institutions in accordance with Article 4.1 of Directive 2006/48/CE; 4. Financial market infrastructures: stock exchanges and central counterparty clearing houses; 5. Health sector: health care settings (including hospitals and private clinics) and other entities involved in health care provisions. Ibid.

[101] Council of the European Union, Doc. 13848/14, 3.

[102] Emmanuel G. Baud *et al.*, 'Europe proposes new laws and regulations on cybersecurity', *Lexology*, January 2, 2014, 2, accessed June 16, 2014,http://www.lexology.com/library/detail.aspx?g=1f872876-3d23-44e7-a8f1-92a9be8d080b .

[103] Jeremy Fleming, 'EU, US go separate ways on cybersecurity', *EuroActiv*, March 5, 2013, 2, accessed June 16, 2014,http://www.euractiv.com/specialreport-cybersecurity/eu-us-set-different-approach-cyb-news-518252 .

[104] NATO Cooperation Cyber Defence Centre of Excellence, 'Developments in the European Union: NIS Directive, Data Protection Reform, EP's response to U.S. surveillance', March 31, 2014, 1, accessed June 16, 2014, http://ccdcoe.org/developments-european-union-nis-directive-data-protection-reform-eps-response-us-surveillance.html .

[105] John Higgins, 'Cybersecurity in Europe must remain focused on critical infrastructures', *Digital Europe*, October 20, 2014, 1, accessed November 3,

2014, http://digitaleurope.blogactiv.eu/2014/10/20/cybersecurity-in%C2%A0europe-must-remain-focused-on%C2%A0critical-infrastructures-%C2%A0/ .

[106] John Higgins, 'Cybersecurity in Europe must remain focused on critical infrastructures'.

[107] Pearse Ryan *et al.*, 'EU Network and Information Security Directive', *Society for Computers & Law*, October 24, 2014, accessed November 3, 2014,http://www.scl.org/site.aspx?i=ed39127.

[108] Scott J. Shackelford & Amanda N. Craig, 'Beyond the New 'Digital Divide': Analizing the Evolving Role of National Governments in Internet Governance and Enhancing Cybersecurity', *Stanford Journal of International Law* 50 (2014): 182.

[109] Scott J. Shackelford *et al.*, 'Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices', *Texas International Law Journal* 50 (2015): 305, 340.

[110] Jay P. Kesan and Carol M. Hayes, 'Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals', *Michigan State Law Review* 5 (2014): 1474, 1537.

[111] Jay P. Kesan and Carol M. Hayes, 'Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals', 1542.

[112] The White House, Office of the Press Secretary, 'Securing Cyberspace - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts'.

[113] Jay P. Kesan and Carol M. Hayes, 'Creating a "Circle of Trust" to Further Digital Privacy and Cybersecurity Goals', 1542.

[114] Robert K. Palmer, 'Critical Infrastructure: Legislative Factors for Preventing a "Cyber - Pearl Harbor"', *Virginia Journal of Law and Technology* 18 (2014), 289, 350.

[115] Jeremy Fleming, 'Cyber security directive held up in face of 'Wild West' Internet', *EuroActiv*, April 1, 2015, accessed November 9, 2015,http://www.euractiv.com/sections/infosociety/cyber-security-directive-held-face-wild-west-internet-313431 , noting that countries like UK, Sweden and Ireland, which host large US-based internet concerns, are leading efforts to minimize the involvement of such companies within the scope of the directive.

[116] Jennifer Baker, 'Cybersecurity? Nothing to do with us, mate - Google and Facebook', *The Register*, November 12, 2014, accessed November 9, 2015, http://www.theregister.co.uk/2014/11/12/cybersecurity_nothing_to_do_with_us_mate_google_facebook_yahoo/ , recalling that the Computer and Communications Industry Association (CCIA) wants the NIS Directive to exclude internet enabling services and focus on 'truly critical infrastructure'

[117] Council of European National Top Level Domain Registries , 'NIS Directive stumbling ahead', October 14, 2015, accessed November 9, 2015,https://centr.org/news/10-14-2015/4468/nis-directive-stumbling-ahead , stating that so-called digital service platforms such as Facebook, ebay, Paypal, etc. will likely be subject to "light touch" regulation. Luke Russell, 'Update on the network and information security directive', July 16, 2015, accessed November 9, 2015, http://www.blakemorgan.co.uk/training-knowledge/articles/2015/07/16/update-network-and-information-security-directive/ .

[118] European Commission, 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', SWD (2013) 32 final, 7.2.2013, 47.

[119] Scott J. Shackelford & Amanda N. Craig, 'Beyond the New 'Digital Divide', 140.

[120] EuroWire, 'EU Cyber Security Policy in the Age of Snowden', January 2014, accessed September 15, 2014,http://www.bfna.org/sites/default/files/publications/EuroWire%20Jan%202014.pdf .

[121] EuroWire, 'EU Cyber Security Policy in the Age of Snowden', 3.