Cyber Security in International Law

Table of Contents

1. Cyber Security ........................................................................................................................................... 2
   1.1 (Absence of a) Definition .................................................................................................................. 2
   1.2 Cyber Threat Landscape ..................................................................................................................... 3
2. International Legal Framework for Cyber Security ................................................................................. 4
   2.1 Political Agendas and International Law ......................................................................................... 4
   2.2 Global Legal Efforts Addressing Cyber Security ............................................................................. 6
      2.2.1 United Nations: Group of Governmental Experts ...................................................................... 6
      2.2.2 Multilateral Treaties: Existence of Security Provisions ............................................................ 8
   2.3 European Legal Efforts Addressing Cyber Security .......................................................................... 10
      2.3.1 Council of Europe: Budapest Convention ................................................................................. 10
      2.3.2 Legal Instruments of the European Union ................................................................................. 12
   2.4 Other Supra-State Legal Efforts Addressing Cyber Security ......................................................... 16
      2.4.1 NATO: Tallinn Manual ............................................................................................................... 16
      2.4.2 Asian Supra-State Legal Efforts ............................................................................................... 17
3. Self-Regulation and International Legal Standards ............................................................................. 18
   3.1 Critical Internet Infrastructure Rules ............................................................................................... 18
   3.2 Acceptance of International Legal Standards .................................................................................. 20
      3.2.1 Concept of Global Public Goods ............................................................................................... 20
      3.2.2 Concept of Shared Spaces ......................................................................................................... 21
      3.2.3 Concept of Responsibility ........................................................................................................... 21
4. Outlook ....................................................................................................................................................... 22
The Internet as the most important global “infrastructure” is an environment in which international law, with all its perplexities, needs to be coherently and effectively applied. Yet the current approach of politicians, scholars and practitioners shows a pertaining reluctance to embrace the challenges posed by global cyber security governance of the biggest international electronic network.

1. Cyber Security

1.1 (Absence of a) Definition

The first step to framing the issue of security in cyberspace is to understand concretely what is meant by the term cyber security. This appears to be a challenging endeavor since, to date, no standard or universally accepted definition of the term exists. To make things more complex, there is no clear consensus on the exact meaning of the term, nor is there even an agreement on its spelling. On that issue, the Internet Society remarked that “as a catchword, cybersecurity is frighteningly inexact and can stand for an almost endless list of different security concerns, technical challenges, and ‘solutions’ ranging from the technical to the legislative”.

The definition of the International Telecommunication Union (ITU) sees cyber security as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets”. Organizations’ and user’s assets include in particular “connected computing devices”. According to the ITU, the ultimate goal of cyber security is to ensure that the security properties of organizations’ and users’ assets are attained as well as maintained against relevant security risks in the cyber environment. General security objectives include those of (i) confidentiality, (ii) integrity, and (iii) availability (also known as the CIA triad in the information security industry). Confidentiality means that information is not improperly disclosed to unauthorized individuals, processes, or devices. Integrity refers to information being protected against unauthorized modification or destruction without authorization. Availability assesses the timely and reliable access to data and information for authorized users.
Cyber security is close to other concepts, such as “Information Security” and “ICT Security”; these terms are often used interchangeably. The International Standardization Organization (ISO) defines Information Security in its standard ISO 27000 as the preservation of confidentiality and availability; ICT Security is a part of it by way of application of information and communication technologies for storage and transfer. Cyber security extends ICT Security by protecting not only information but also assets that are non-information based and vulnerable to ICT threats.

1.2 Cyber Threat Landscape

Possible Categorization: One way to start a discussion about cyber security can be the identification of the threats that challenge it. Hereinafter, the contemporary cyber threat landscape will be described by using a linear approach that distinguishes threats by (i) threat agents, (ii) threat tools, and (iii) threat types. While such categorization is useful for certain legal qualifications, it does not (aim to) paint a comprehensive picture of the very complex nature and characteristics of cyber threats, as it in particular neglects the extent to which categories overlap and produce interwoven effects.

Threat Agents: A wide array of external and internal agents threatens cyber security. Threat agents can be sophisticated or non-sophisticated. They include Nation States, profit-driven cyber criminals, criminal organizations, hackers (black, grey or white hats), extremists and insiders; obviously, a given agent can belong to more than one category.

The motivations of threat agents vary significantly. Agents act for political reasons (e.g. destroying, damaging, disrupting, or taking control of targets, engaging in cyber espionage or political protest). They may further have financial (e.g. stealing valuable personal or financial data, such as the social security numbers or credit card numbers that can be used for identity theft and fraud) as well as socio-cultural motivations (e.g. engaging in attacks with philosophical goals or for purposes of publicity, curiosity or ego).

Threat Tools: Threat agents typically leverage similar threat tools. The basic security breach tools encompass malware and its variants (ransomware, viruses, worms, Trojan horses, etc.) and botnets. Malware is a general category referring to any code or
software covertly installed on a device without authorization. It includes malicious code designed for the purpose of damaging, disrupting, or generally inflicting some kind of illegitimate action on data, systems, or networks. A further variation is ransomware, a type of malware that that restricts access to the infected device or system in some way. While a ransomware attack leaves the system working with all data present, due to the integrity compromise, it causes certain files to no longer be usable. Cyber attackers then demand a ransom, generally in Bitcoin, to restore the original integrity of the files. Botnets usually consist of command and control (C&C) servers and networks of computers infected by malware that can be remotely managed. So far, malware represented the number one cyber threat. Ransomware was and, according to industry experts, will remain a major and rapidly rising threat. Botnets (“botnet-for-hire” business model) as main elements in cyber crime consumerization were also reported to feature among the preferred weapons of cyber criminals.

**Threat Types:** Threats to cyber security involve threats concerning information modification or misuse, information destruction, unauthorized access, data breach, data theft and denial-of-service (DoS). Although all facets of the mentioned CIA triad are threatened by cyberattacks, McAfee Labs predicted that the threats to integrity of systems and data would constitute one of the most significant new vectors of attack. This is because, as described by McAfee Labs, “confidentiality and availability attacks are loud, brute, and obvious. They break things and expose data – causing embarrassment, inconvenience, and some losses. Integrity attacks are stealthy, [and] selective, […]. Instead of doing damage or making off with vast amounts of sensitive data, they instead focus on carefully changing particular elements within transactions, communications, or data to gain a significant benefit”.

2. **International Legal Framework for Cyber Security**

2.1 **Political Agendas and International Law**

Cyber security is now routinely cited and consistently placed on the top of political agendas. Governments from around the world have endeavored to secure cyberspace and its systems. Particularly, they have devised and adopted countless cyber security strategies and corresponding regulations. Examples are China with its Cybersecurity

In addition, international law also attracted more attention during the last few years. Nation States have undertaken (at least partly concerted) efforts to implement new or enhanced multilateral cyber laws and regulations. This is done with the objective to adapt to the shifting environment and address the need for coordinated action created by the inherently transnational nature of the issue and the resulting need to achieve cyber security on a global level.

However, despite the flurry of activities and initiatives relating to cybersecurity, there is, for the time being, no truly universal and comprehensive instrument in this field. Rather, the global picture is one of fragmented membership of instruments at the international and regional level and of a patchwork quilt of sectoral laws at national levels. Amidst this patchwork of protection, there appears to be some confusion as to what legislation to allude to. Nonetheless, some legal instruments that address the challenges of cybercrime and cyber security do exist.

Security in general (not cyber security in particular) has been a regulatory topic for quite some time in multilateral treaties for example governing telecommunications or international trade: (i) The term “security” is defined in numerous Recommendations of the International Telecommunication Union (ITU); the definitions are not identical, but in essence consistent. (ii) The international trade law (GATT and GATS of the World Trade Organization [WTO]) refers to “essential national security interests” such as military establishments, nuclear fission and fusion, wartime or other emergency in international relations; attempts to fructify these notions also for cyber security by broadening their scope can now be seen.

Hereinafter, the global legal efforts addressing cyber security will first be discussed, followed by the more detailed considerations to the European and to other supra-State legal instruments having been put in place during the last two decades.
2.2 Global Legal Efforts Addressing Cyber Security

2.2.1 United Nations: Group of Governmental Experts

A global concern such as cyber security principally merits the attention of global organizations, in particular the United Nations (UN) and its – information transmission oriented – sub-organization, the International Telecommunications Organization (ITU). Indeed, the UN traditionally calls upon experts to facilitate its work in various areas of international law. In respect of cyber security, the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) was appointed more than 15 years ago. The UN GGE was unique in both, the broad scope of its mandate and the high expectations for its results. Thus far, several Groups of Governmental Experts have been working on “existing and potential threats from the cyber-sphere and possible cooperative measures to address them”.

The first UN GGE, dating back to 2004, consisted of 15 members and failed to produce a consensus report due to two crucial unresolved policy questions: (i) The scope of the needed debate, in particular whether the focus should be only directed to infrastructure management or put also on content, especially whether regulating transboundary flow of information was a national security issue, and (ii) the need to include some language emphasizing new threats originating from state exploitation of new information and communication technologies (ICTs) for military and security purposes.

The second UN GGE (2009/2010) produced a report recommending a dialogue on norms for State use of ICTs to reduce risk and protect critical infrastructure and “confidence-building and risk-reduction measures”.

The third UN GGE (2012/2013) advocated for international law and in particular the UN Charter to be applicable to cyberspace, which should remain “open, secure, peaceful and accessible”. It also confirmed that States are sovereign to regulate cyberspace and have the territorial jurisdiction over the cyberspace infrastructure located within their borders. Furthermore, it emphasized the need to respect human rights online, arguing that “state efforts to address the security of ICTs must go hand-in-hand with
respect for human rights and fundamental freedoms” while “States must not use proxies to commit internationally wrongful acts and must ensure that their territories are not used by non-state actors for unlawful use of ICTs”.

The fourth UN GGE (2015) produced a comprehensive consensus report on norms, rules or principles of the responsible behaviour of states in cyberspace as well as on confidence building measures, international cooperation and capacity building. Its findings confirmed four principles of the international law’s application to cyberspace:

(i) “In their use of ICTs, States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States.

(ii) Existing obligations under international law are applicable to State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms.

(iii) States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.

(iv) The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour.”

The fifth UN GGE (2016/2017) faced a significant challenge, transposing these general principles into more detailed obligations. It was to tackle cyberspace, Internet governance and cyber security – points of particular contention in the era of rising international tensions on cyber security, the ambiguity of legal qualifications of cyberattacks and the limits of States’ due care in preventing foreign harm originating from their territory through computer networks. The UN GGE operated with traditional intergovernmental tools in a multistakeholder domain, seeking intergovernmental consensus where governments are no longer the only rule-makers. But the efforts failed, an agreement on cyber security principles could not be achieved. The failure of the last UN GGE was
due to two factors, namely (i) the increasing political tension related to the attribution of cyberattacks, fuelled by mutual accusations and a low willingness to share expertise on the part of all major players, and (ii) the lack of consideration for non-State partners in Internet governance norm-making.

Notwithstanding the previous problems the UN General Assembly decided in late 2018 to continue the UN GGE and to establish a new open-ended group. These two groups should endeavor and they are mandated to further study norms, confidence-increasing measures and capacity-building efforts, also taking into account their effective implementation. First results are not expected to be published before 2021. Therefore, it remains uncertain whether the world community will be able to witness the emergence of a single legal regime for the regulation of cyber security.

2.2.2 Multilateral Treaties: Existence of Security Provisions

As mentioned, multilateral treaties addressing the cross-border rendering of goods or services usually contain specific security provisions. Two examples are analyzed hereinafter.

(i) International Telecommunication Union (ITU): The International Telecommunications Regulations (ITR) of the ITU show, how difficult the concretization of the term “security” can be in the international environment. This term was intensively debated during the World Conference on International Telecommunications (WCIT) in Dubai (December 2012). On the one hand, particularly by the Western countries, it was argued, that “secure” would mean “robust” and “safe”, i.e. the technical functioning has been considered to be the main purpose of security. On the other hand, some countries being organized more hierarchically expressed the opinion that security should also include the notion of “public order”; this approach envisaged to allow Nation States to intervene based on policy considerations.

Finally, a majority of the WCIT participants agreed to the following wording of Article 6.1 ITR: “Member States shall individually and collectively endeavor to ensure the security and robustness of international telecommunications networks in order to achieve effective use thereof and of an avoidance of technical harm thereto, as well as the
harmonious development of international telecommunication services offered to the public”. The notion of “public order” or “public policy” has not been literally taken up by the ITR, but emphasis was put on the technical harm. Therefore, Nation States do have a relatively broad leeway in connection with the implementation of Article 6.1 ITR. This example shows that the scope of the term “security” remains subject to unclear interpretative approaches.

(ii) World Trade Organization (WTO): In international trade law (particularly in the regulatory framework of the GATT, the GATS and the General Procurement Agreement of the WTO), the already mentioned term of “essential security interests” is used; if such an interest is justifiably invoked by a Nation State, cross-border trade barriers can be implemented. However, since such barriers contradict the spirit of international trade law, the interpretation of the respective notion of “security” as an objective criterion becomes crucial. Two elements appear to be relevant: (i) The interest must relate to the security of a Nation State and (ii) it has to be qualified as “essential”. The challenges particularly occur in connection with the inclusion of non-economic military or political motives.

For quite some time it was assumed that Nation States do have a wide discretion, only limited by the abuse threshold, i.e. WTO Members would be allowed to define what they consider necessary for the protection of their national security interests. However, in the recent case “Russia – Traffic in Transit” the WTO Panel advocated for a more nuanced approach by recognizing that the existence of the enumerated legal conditions is not self-judging; rather it must be assessed whether the national measure is necessary for the protection of the State’s essential security interests in response to the existence of the legal conditions. Therefore, even if necessity is subjective, judicial review may address whether the State is acting in good faith in the interpretation of the external threats, the maintenance of law or the public order. Justified interventions cannot only encompass measures against actual threats but also cover preventive actions. Nevertheless, according to legal doctrine, the security exception should be considered as the last resort to ensure the national policies sphere in case of an international emergency.
2.3 European Legal Efforts Addressing Cyber Security

Looking at the supra-State level, Europe appears to be the most advanced region in adopting cross-border regulations in the cyber security field. As important legislative instruments (i) the Budapest Convention of the Council of Europe and (ii) several regulatory activities of the European Union are to be addressed.

2.3.1 Council of Europe: Budapest Convention

The Budapest Convention of the Council of Europe was adopted in 2001 and entered into force in 2004. It is considered to be the oldest binding and widest adopted legal instrument in the field of cybercrime. The Budapest Convention is open to worldwide membership. To date, 63 States have ratified the Convention, including several important non-EU Members, for example Argentina, Australia, Canada, Chile, Israel, Japan and the United States. Additionally, four States are signatories and some others have been invited to accede. Despite this wide adoption, the Convention is not yet truly global. Importantly, it does in large part not extend to developing countries, which means that a significant portion of Internet users do not fall within its scope.

Objectives and Content

As set forth in the Preamble, the main objective of the Budapest Convention is to pursue a “common criminal policy” against cybercrime, by “adopting appropriate legislation and fostering international co-operation”. The aim of the Convention is to “deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data” by providing for the criminalisation of such conduct and by facilitating detection, investigation, and prosecution at the domestic and international level.

Pursuant to the explanatory Report of the Budapest Convention, the rationale for a common criminal policy is that, while the “most effective means” to prevent unauthorised access is “effective security measures”, a comprehensive response must also include deterrence, i.e. “the threat and use of criminal law measures”.

10
The Budapest Convention provides for four categories of substantive offences, including offences against (i) the confidentiality, integrity and availability of computer data and systems (Art. 2-6) and (ii) computer-related offences (Art. 7-8). The explanatory Report specifies that the criminal offences defined under Articles 2-6, which include hacking and computer trespass, are intended to protect the confidentiality, integrity and availability of computer systems. As such, the importance of (protecting) the CIA triad is clearly reflected in the Convention. As to the concept of computer systems, it is defined under the Convention as meaning “any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data” (Art. 1).

In terms of scope, the categories of offences of the Budapest Convention do not encompass the full range of cybercrimes. This may be attributable to the fact that certain offences were likely not anticipated (which is unsurprising since the Convention was drafted in the nineties of the last century) but also that international consensus could not be reached with respect to certain offences. Even so, the Convention provides for the possibility to supplement or amend the Convention (Art. 46). Further, other bodies may address the substantive offences of the Convention, provided that such activity does not conflict with the Convention. In practice, this last provision provides the means for Member States to update their cybercrime legislation, despite the Convention remaining static.

As regards the broader issue of cross-border cooperation, the Budapest Convention requires parties to cooperate with each other “to the widest extent possible” for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence (Art. 23). The goal of effective cross-border cooperation is to “minimize impediments to the smooth and rapid flow of information an evidence” on an international level. This general obligation to cooperate is further reaffirmed in subsequent provisions, which lay down the principles of extradition (Art. 24), mutual assistance (Art. 25) and spontaneous information (Art. 26), which entitles parties to receive relevant data without a prior request.
Assessment

The Budapest Convention was the first (ambitious) attempt to harmonize the legal framework for combatting cybercrime. Despite its role in providing an internationally recognized framework for international harmonization and its influence on a great deal of the current EU cybercrime legislation, almost two decades after its coming into force, the Convention has been described by its critics as largely outdated and in great need of reform. Various reasons have been cited for such claimed obsolescence, including the fact that the Convention is based on types of offenses which originated at the time of its drafting (i.e. the late 1990s) and therefore does (logically) not take into account new attack tools (such as botnets and ransomware). Further, the Convention does not specifically mention virtual economic crime, although it purports to govern cybercrime. As a result, there have been calls for a general revision of the Budapest Convention or even the adoption of a new (and truly) universal treaty on cybercrime, for instance at the UN level.

2.3.2 Legal Instruments of the European Union

2.3.2.1 Network and Information Security Directive

The European Union (EU) has decided to combat cybercrime and bolster cybersecurity through various actions. As such, the EU has designed and adopted the following recent instruments and strategies: (i) the hereinafter discussed legal instruments in the cyber security field, (ii) the General Data Protection Regulation (GDPR) being in force since end of May 2018 and (iii) the EU Digital Single Market strategy (DSM) (which synthetizes in particular the initiatives on security and data protection).

Policy Context

Already in 2001, the European Commission had highlighted the increasing importance of network and information security (NIS) in its Communication Network and Information Security: Proposal for a European Policy Approach. In 2004, the European Network and Information Security Agency (ENISA) was established, with the objective to promote "a culture of network and information security for the benefit of citizens,
consumers, business and public sector organisations in the European Union”. ENISA was mainly tasked with tracking information security risks, facilitating cooperation and information-sharing between public and private sector entities, and assisting member states in their development of industry-specific cybersecurity strategies.

**History of the NIS Directive:** In 2006, the European Commission adopted a “Strategy for a Secure Information Society”, with the goal to develop a culture of NIS in Europe. The main elements of the 2006 strategy, including the security and resilience of ICT infrastructures, were endorsed in a European Council Resolution. In line with the 2006 strategy, in 2009, the European Commission adopted a “Communication on Critical Information Infrastructure Protection”, which focused on the protection of Europe from cyber disruptions by enhancing security and resilience. In 2012, the European Commission held an online public consultation on “Improving NIS in the EU”. The key outcome of the consultation was the wide support by stakeholders for improving NIS across the EU.

In 2013, the European Commission published the “Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace”. This Strategy sets forth the EU’s approach on best preventing and responding to cyber disruptions and attacks. It does not centralize supervision, but rather encourages Member States to organize and respond to cyber threats at the national level. The Strategy sets forth a series of actions aimed at enhancing cyber resilience and reducing cybercrime, among other things. It also grants ENISA the power to cooperate with the public and private sector in order to advance the adoption of NIS standards and support business activities with the development of guidelines that reflect industry best practices.

In conjunction with the release of the Strategy, the European Parliament and European Council proposed a “Network and Information Security Directive” to ensure a high common level of network and information security standards among Member States. Prior to the introduction of the NIS Directive Proposal, the European Commission had noted the absence of any effective mechanism at EU level for effective cooperation and collaboration and for trusted information sharing on NIS incidents and risks among Member States. Therefore, the European Commission had alerted to the risk of uncoordinated regulatory interventions, incoherent strategies and divergent standards, resulting in insufficient protection across the EU. On 7 December 2015, the European Parliament and the European Council reached a political agreement on the European
Commission’s proposed measures to increase online security in the EU. On 18 December 2015, the final compromise draft of the NIS Directive was released. On 16 July 2016 the European Parliament and the Council formally adopted the NIS Directive, obliging the Member States to transpose the Directive into their national laws by 9 May 2018.

Objectives and Content

As mentioned, the NIS Directive is the first EU-wide legislation on cyber security. Its core objectives are to achieve minimum regional (EU) harmonization and to make the online environment more trustworthy, which ultimately supports the establishment of the Digital Single Market.

The NIS Directive explicitly refers to the above mentioned CIA triad in its definition of NIS security, which provides that “the ability of networks and information systems to resist, at a given level of confidence, any action that compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by or accessible via that network and information systems” (Art. 4 [2] NIS Directive).

The Directive sets forth the following main objectives and measures to bring about the aimed high common level of NIS in Europe (Art. 1 NIS Directive).

(i) **Improved National Cybersecurity Capabilities**: Member States are required to adopt a national cyber security strategy (Art. 7 NIS Directive, NIS Strategy). This includes creating a policy and a regulatory environment for information security. The NIS Directive further requires Member States to establish institutional capacities. As such, Member States must designate national competent authorities for the implementation and enforcement of the NIS Directive (Art. 8 NIS Directive) as well as a national Computer Security Incident Response Teams (CSIRT) responsible for handling incidents and risks (Art. 9 NIS Directive).

(ii) **Improved EU-level Cooperation**: the NIS Directive creates a Cooperation Group with the objective to support and facilitate strategic cooperation and the exchange of information between Member States (Art. 11 NIS Directive).
Security and Incident Notification Requirements: in order to “promote a culture of risk management and ensure that the most serious incidents are reported” (Recital NIS Directive), the NIS Directive imposes security and incident notification requirements on two group of entities, i.e. (A) operators of essential services, and (B) digital services providers. This distinction and differentiated treatment is due to the differences between operators of essential services (which have a direct link with physical infrastructure) and digital service providers (which have a cross-border nature).

The success of the NIS Directive cannot yet be assessed since the national implementation only happened a year ago. But it can be positively said that the role of ENISA gained importance and that the national CSIRT attempt to improve the cross-border cooperation.

### 2.3.3.2 Cyber Security Act of the European Union

In September 2017, the European Commission adopted a “Cyber Security Package” with the objective to further enhance resilience to cyber threats in the EU. This package was building on the existing instruments, but also encompassing new initiatives. In order to foster the operational implementation of the NIS Directive, further measures have been proposed. A second legislative activity included a regulation on ENISA, the “EU Cyber Security Agency”; the Commission is intending to strengthen its role by updating its mandate and building capacities needed to develop a certification scheme.

The certification is subject to the Cyber Security Act which was discussed by the EU institutions mainly during the year 2018 and has been adopted in spring 2019. The Cyber Security Act provides for a “Cyber Security Certification Framework”, designed to accelerate the growth of the Digital Single Market. In view of the increasing number of cyber incidences across Europe, the new legislative instrument implements security certifications schemes covering aspects of confidentiality, integrity and availability, privacy and particular aspects such as the provision of mechanisms for secure software updates. Under the new framework, cyber security certification schemes will include the following elements: (i) products’ and services’ categories and service; (ii) specification of the cyber security requirements; (iii) intended assurance levels; (iv) criteria
for certification; (v) evaluation criteria and methods used; (vi) conditions of granting marks and labels.

Specific products’ and services’ categories are industrial automation control systems, connected and automated cars, electronic health systems and smart grids. Evaluation criteria should describe the methods used to demonstrate the conformity of products and services with the certification criteria. ENISA’s tasks under the Cyber Security Act encompass (i) the development and implementation policy and law, (ii) the capacity-building, (iii) the operational cooperation at EU level, (iv) the support and promotion of the EU cyber security certification framework, (v) tasks related to knowledge and information, awareness-raising and education, and research and innovation, as well as (vi) the international cooperation. In addition, a Cyber Security Certification Group (CCG) will be established, consisting of national supervisor authorities from all Member States.

2.4 Other Supra-State Legal Efforts Addressing Cyber Security

2.4.1 NATO: Tallinn Manual

Among the State-led actions targeting cyber security challenges the most prominent documents have been adopted by the North Atlantic Treaty Organization (NATO), an intergovernmental organization of Western countries focused on armed conflicts and international peace. At the Security Summit in 2016, NATO recognized cyberspace as the fifth warfare domain and confirmed that a cyberattack against any of its allies would be considered an act of war. A particularly important outcome of NATO’s cyber security focus was the Tallinn Manual, offering a first comprehensive study of international law applicable to cyberspace. The Tallinn Manual is now available in its second edition. It defines critical infrastructure as all systems and assets, physical and virtual, within a Nation State’s jurisdiction that “are so vital that their incapacitation or destruction may debilitate a State’s security, economy, public health or safety or the environment.” It also defines the term “cyber infrastructure” covering “communications, storage, and computing resources upon which computer systems operate”.

16
The Tallinn Manual is not binding on the NATO Members but it provides for a set of cyber norms during times of war. According to Rule 81, it is prohibited to attack, destroy, remove or render useless “objects indispensable to the survival of the civilian population by means of cyber operations”. The Tallinn Manual should cover objects indispensable to the survival population even if neither the Internet nor its infrastructure is considered to be part of existing customary law. The expression “depending on circumstances” includes “cyber infrastructure indispensable to the functioning of electrical generators, irrigation works and insulations, drinking water insulations and food production facilities”. However, the observations are to be considered only with reference to a time of war.

2.4.2 Asian Supra-State Legal Efforts

The Shanghai Cooperation Organization (SCO) is an intergovernmental body created by China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan in 2001. Apart from the cooperation in areas such as trade and economy as well as science and technology, the SCO is paying particular attention to the cooperation in the field of ensuring the international information security. In 2011, four of the SCO Members submitted a proposal for an International Code of Conduct for Information Security to the United Nations Secretary-General; later, in 2015, all five SCO Members presented a revised version of the Code to the UN General Assembly.

The politically most prominent SCO Members, namely China and Russia, signed a further bilateral Information Security Agreement having been heralded as a “non-aggression pact” between the two countries in cyberspace. Particularly, China and Russia pronounced support for the concept of “cyber sovereignty” being a shared strategic interest that contrasts with the U.S. advocacy for “cyber freedom”. This concept was emphasized by the Chinese President Xi Jinping at the 6th BRICS summit in 2014 and later at the Wuzhen World Internet Conference in December 2015.

However, the actual Sino-Russian cyber security cooperation seems to be relatively limited. The first Russia-China Information and Communication Technologies Development and Security Forum, held in Moscow in April 2016, had the main focus of implementing Internet regulation and protecting cyber sovereignty. Some commentators
express the opinion that the bilateral ties between China and Russia will hardly lead to an alliance, rather, the cooperation is a “marriage of convenience” (defined in relation to the United States). Therefore, the intensity of the supra-State efforts in cyber security matters appears to be less intensive in East Asia than in the NATO.

3. Self-Regulation and International Legal Standards

3.1 Critical Internet Infrastructure Rules

The normative framework of the Internet was originally mainly based on self-regulation; since the famous declaration of John Parry Barlow (1996) advocating for the “Independence of Cyberspace” many netizens assumed that State regulations would not be relevant in this new environment. Even if this assumption did not realize, at least in the context of the critical Internet resources, technical rules of private organizations still play an important role.

As mentioned, the current Internet governance landscape was originally designed as the effect of bottom-up governance models, rooted strongly in the technical community, for example the Internet Society (ISOC) or the Internet Engineering Task Force (IETF) with its “Requests for Comments” (RfC), community-developed common standards voluntarily followed by its members: Internet service providers or software developers. While “security by design” remains a common paradigm within both, ISOC and IETF, there is no connection to be made between this extra-legal, community-based rule making approach and the hard norm-setting models of States. While ICANN, ISOC, and IGF have been attending to the issue, this communications’ gap holds crucial relevance for the development of any effective international cyber security policies and must be addressed by whatever model of global cyber security. There can be no effective cyber security policy developed solely at governmental level, without strong presence of the technical community and vigilant input from civil society.

An important intergovernmental attempt to directly address the issue of Internet’s infrastructure at the policy level is the Council of Europe (CoE) Report of 2009 addressing "Internet Governance and Critical Internet Resources”. It identified “Critical Internet
Resources” (CIR) that require particular care from the international community to ensure the free and reliable flow of information online. According to the CoE, the CIR include: root servers, Domain Name System, Internet Protocol and the Internet “backbone structures”, as well as Internet Exchange Points (IXPs). The CoE emphasizes the need to secure universal broadband access and network neutrality and linked the need to protect CIR with the existing critical resources perception, indicating the Internet itself as a “critical resource” and arguing that for it to remain “sustainable, robust, secure and stable” it must be protected “in the same way than other critical common resources are protected”.

Critical infrastructure protection as provided by existing national regimes and international cooperation programs, such as the European Programme for Critical Infrastructure Protection (EPCIP), usually encompass networks fundamental to the daily operation of any modern day society: water and energy supply, mass transportation, health and emergency services and alike. The last and newest category included in Annex II to the NIS Directive covers “digital infrastructures” and includes (i) Internet exchange points (IXPs), (ii) Domain Name System service providers and (iii) Top Level Domain name registries. These categories mirror the current EU approach to cybersecurity, viewing crucial Internet infrastructures as part of the European critical infrastructures ecosystem. Effectively they all require the same level of protection from their operators, including e.g. security due diligence measures and risk assessments. While other services or networks might be considered critical by different States or regions (just to mention those countries which include election infrastructures in their critical infrastructures list), the NIS Directive serves as a relevant point of view for the discourse on international (as opposed to national) approaches to critical infrastructure protection.

This latest development in EU cyber security policy is interesting for two reasons. First, it lists “digital infrastructures” together with services well-recognized as parts of national critical infrastructures, such as water supply or transportation. It therefore represents a well deliberated policy decision by the 28 EU states to use the existing resilience network, represented by e.g. the European Programme for Critical Infrastructure Protection (EPCIP), for key Internet resources: IXPs, DNS operators and TLD registries. Interestingly, the EU debate on the NIS Directive was prolonged not only due to
the inclusion of “digital infrastructures” as critical networks, but also because obligations similar to those imposed on critical infrastructure operators were to apply also to “digital services” offered within the “digital marketplace”, namely to online search engines and cloud computing services.

3.2 Acceptance of International Legal Standards

Cyber security can only be reasonably warranted if the international community is ready to accept the some basic and common legal standards being applicable around the globe. Several theoretical models have been developed so far; hereinafter the concepts of global public goods, of shared values and of responsibility will be further analyzed.

3.2.1 Concept of Global Public Goods

One of the starting points for a discussion on protecting cyber security could be the concept of “global public good”. Although not perfectly aligned to the needs of cyber security and the network’s architecture, it is worth a closer look. A complementary concept of “critical infrastructures” and their protection can serve as another point of reference. Ideally, global public goods are those which benefit humanity as a whole; accordingly, these goods should be advantageous to (i) more than one group of countries or geographic regions, to (ii) a broad spectrum of the global population, crossing population segments, and (iii) to present generations without jeopardizing the ability of future generations to meet their own needs.

The idea of guaranteeing cyber security as a public core of the Internet or as a “global public good” can be perceived as a derivative of a policy concept: The ambiguous notion of “global public goods”, once generated in the era of globalization, is derived from the economic writings of Paul Samuelson on “public goods”. It refers to all globally available goods that are non-rivalrous (consumption does not influence the quantity available to others) and non-excludable (their use cannot be prevented); the examples of global public goods include knowledge as well as the common heritage of mankind.
From an international law perspective, global public goods theories are not totally new. The idea of a certain “communality” already lies at the core of Roman law concepts of “ius cogens” or “erga omnes”; similarly, the “public interest” concept, peremptorily imposing binding obligations on States, has a similar foundation. However, global public goods theories involve a broader approach that takes political economy implications into account besides legal aspects.

3.2.2 Concept of Shared Spaces

International cooperation on critical infrastructure protection is not the only analogy to be drawn from existing legal frameworks. Also, for example, the concept of shared spaces, to be used by all States in a uniform, non-harmful way is not new to the international community, international relations and international law. Areas of international law that can be used for reference with regard to guaranteeing cyber security include: (i) the law of the sea; (ii) air and space law; (iii) diplomatic and consular law; (iv) international human rights law; (v) international telecommunication law; (vi) environmental law; (vii) international trade law; (viii) antiterrorist laws and policies. While each of these legal regimes offers interesting insights that can be useful to Internet resilience, a concise and general assessment, derived from all those areas of international law and relations, is still outstanding.

The Tallinn Manual 2.0 indicates that there are overarching international law principles relevant to all those specified regimes: (i) sovereignty, (ii) jurisdiction, (iii) state responsibility, and (iv) due diligence. While sovereignty and the matrix of jurisdictional principles remain an unresolved challenge for critical infrastructure protection, subject to enhanced debate and still far from consensus, the two other principles, namely state responsibility and due diligence can be easily applied to the biggest international open networks and their key components.

3.2.3 Concept of Responsibility

The law on State responsibility is perceived as a secondary regime, applicable to all other specified international law norms imposing obligations upon States. Once an international obligation of a State is breached – be it an obligation of conduct or one of
result – the consequences provided for in the law of State responsibility entail. The principle of due diligence implies a State’s duty to act with due care in preventing a violation of international law. Indications of what is meant with “due care” in particular circumstances are to be derived from the law and practice within individual areas of State practice and international relations.

Analogically, a due diligence standard for cyber security could serve as a point of reference for State’s responsibility in respect of an omission resulting in transboundary harm, e.g. a malfunction of a foreign power plant caused by a cyberattack initiated or an incident generated from within State territory. The existing community standards with regard to good business practice within each of the specific sectors (e.g. root zone operation, IXP operation, DNS and TLD management) could be referred to by both, the concerned State in filing its claims and the adjudicating court. Due diligence appears in all the mentioned legal regimes, and is also relevant for the law on neutrality in armed conflicts, which “is, in principle, applicable to cyberspace”. In other words, “governments should closely cooperate in a continuing effort to arrive at an operable consensus that takes into consideration global interoperability, network stability, reliable access and cybersecurity due diligence.

4. Outlook

Cyber security is an objective that should eliminate or at least minimize risks caused by an inappropriate use of international electronic infrastructures. Risk is the function of the likelihood of an adverse event, interacting with the magnitude of harm upon the occurrence of an adverse event. Precautionary measure can be taken by the private actors, for example by way of standardization, as the network security provisions of ISO/IEC 27001 show, or by national, supra-State or international legislators. Furthermore, it is possible to implement the administration of the regulatory framework through (i) private institutions with regulatory functions, (ii) hybrid intergovernmental-private arrangements, (iii) distributed regimes of regulators in cooperative schemes, (iv) collective action by transnational networks between officials or (v) formal international organizations.
Previous experience in the field of cyber security has shown that the traditional international law approach operating on State level through multilateral treaties, thereby failing to directly address duties of private actors, is hardly able to cope with the challenges of combatting cyberattacks (in different forms). The inclusion of various stakeholders into a new regulatory framework appears to be unavoidable. This attempt has been undertaken by Microsoft in 2017 when suggesting to adopt an international treaty to guarantee the peaceful use of cyberspace. The proposal to develop a “Digital Geneva Convention” referred to the “Treaty on the Non-Proliferation of Nuclear Weapons” and the “Treaty on Chemical Weapons” as examples of international regimes limiting vital threats to human existence. However, this proposal met the scepticism of many States and it also appears to be unclear to what extent other Internet stakeholders could be included in such an arrangement.

As outlined, so far the (incoherent) patchwork of cyber security regulations does not really correspond to the political needs. The only exception concerns the European Union with the recently adopted (directly or indirectly applicable) legal regime, however, the practical implementation in the EU still needs to become successful. On a global level, further efforts to achieve a better coordinated regulatory framework are required; it is also up to the businesses and the academics to contribute to these efforts with more emphasis.