# Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives

*A. Verhelst, J. Wouters*

**Anne Verhelst** – PhD Researcher in International Law, Leuven Centre for Global Governance Studies and Institute for International Law, KU Leuven and Fellow of Research Foundation – Flanders (FWO); 13 Oude Markt, Leuven, Belgium; E-mail: anne.verhelst@kuleuven.be

**Jan Wouters** – Full Professor of International Law and International Organizations, Director of the Leuven Centre for Global Governance Studies and Institute for International Law, KU Leuven; 13 Oude Markt, Leuven, Belgium; E-mail: jan.wouters@ggs.kuleuven.be

**Abstract**

*The many recent cyber incidents have shown how cybersecurity has entered the realm of international relations. Several international organizations have taken cybersecurity policy initiatives, notably the United Nations (UN) and the European Union (EU). Both organizations aspire to a leading role in enhancing cybersecurity resilience. To date, however, these initiatives have not resulted in much regulation. This article examines which factors make lawmaking and the regulation of cybersecurity difficult at the international level, and whether some of these impediments are shared at the EU legislative level. Are difficulties in regulating cybersecurity embedded in the normative processes at the UN or the EU, or are they inherent to the high-tech phenomenon of cyber? As for the UN, the article looks at the work of the UN Group of Governmental Experts (GGE). While previous reports of the UN GGE seemed to point to an emerging international opinio juris, recent developments in the UN General Assembly (UNGA) show a strongly divided international community. At the EU level, the article discusses the two main legislative initiatives on cybersecurity that have seen the light of day: the 2016 Directive on Network and Information Security and the 2019 EU Cybersecurity Act.*

**Key words:** cybersecurity; global governance; international law; European Union; lawmaking; regulation; policy; UN GGE; Open-ended Working Group; NIS Directive; EU Cybersecurity Act

**For citation:** Verhelst A., Wouters J. (2020) Filling Global Governance Gaps in Cybersecurity: International and European Legal Perspectives. *International Organisations Research Journal*, vol. 15, no 2, pp. 105–124 (in English). DOI: 10.17323/1996-7845-2020-02-07

## Introduction

Over the first two decades of this millennium, cybersecurity has become omnipresent within international relations. Yet, while clearly a policy concern, it has generated very little international regulation up to now. A straightforward reason that partially explains this inertia, is that the scope, nature, meaning, and terminology of cybersecurity are unclear [Futter, 2018, p. 202; Nye, 2016/17, p. 68].[1] There is little general agreement about what cybersecurity entails [European Court of Auditors, 2019], and it seems that different people use the term differently, de-

[1] According to Futter [p. 209], the terminological vagueness is not without practical impact: the definition of cybersecurity in a given context is after all contingent upon what and who is being deterred, how, and whether the attribution of capabilities is possible. "The vague language means that it can be unclear who should

pending on the context [Futter, 2018, p. 205; Kosseff, 2018, p. 995; Kshetri, 2016, p. 3; Schatz, Bashroush, Wall, 2017, pp. 53–7]. This article focuses on cybersecurity *sensu stricto*, excluding a focus on the specific threats of cybercrime [Kshetri, 2016; 2009, pp. 141–4],[2] cyber terrorism [Harrison Dinniss, 2018, pp. 45–50; Ivanov, 2015, pp. 55–69; Fidler, 2015, pp. 10–1] and cyber warfare.[3, 4] This article does not study organizations that have taken policy or legislative initiatives on one of those specific threats.[5] In the United Nations (hereinafter: "UN") context, cybersecurity has been defined by the International Telecommunication Union (hereinafter: "ITU"), a definition which has been further refined by Kshetri: "cybersecurity involves technologies, concepts, policies, processes and practices used to protect assets (e.g. computers, infrastructure, applications, services, telecommunications systems, and information) and the cyber environment from attack, damage and unauthorized access" [ITU, 2008].[6] In the European Union (hereinafter: "EU") context, the following definition is used under the Cybersecurity Act: "cybersecurity means the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats" [EU, 2018, Art. 2(1)].

Many policy initiatives regarding (different (sub)domains of) cybersecurity have been initiated, notably within the UN[7] and the EU contexts.[8] Both organizations aspire to a leading role in enhancing cybersecurity resilience. As both organizations have interesting – but very different – lawmaking processes, and the former constitutes a unique global organization while the latter constitutes a unique type of regional[9] organization,[10] this article will compare the normative initiatives on cybersecurity *sensu stricto* which the two organizations have undertaken.

The overall aim is to discuss how and to what extent global governance gaps on cybersecurity are being filled, by analyzing the most salient recent developments in cybersecurity law

---

take responsibility for ensuring cybersecurity, leading to various legal and practical obstacles in regulating the issue."

[2] Cybercrime can be defined as "a criminal activity in which computers or computer networks are the principal means of committing an offense." Examples include "cyber-theft, cyber-trespass, cyber-obscenity, and cyber-extortions." Some authors and instruments categorize cyberattacks against critical infrastructure under 'cybercrime'. In this article discusses the EU NIS Directive [EU, 2016, *infra* Section IV), which aims to protect critical infrastructure regardless of whether a cyberattack against such infrastructure should be seen as falling under a strict definition of 'cybercrime'. A specific regional instrument dedicated to cybercrime as such is the Budapest Convention on Cybercrime [Council of Europe, 2001]. See also the African Union Convention on Cyber Security and Personal Data Protection [African Union, 2014; Orji, 2018].

[3] For example, Rules 20–95 of the Tallinn Manual 2.0 [Schmitt et al., 2017].

[4] Many initiatives that aim at regulating cybersecurity only address a certain area of its framework, such as the protection of critical infrastructure (e.g. EU NIS Directive), data protection online (e.g. the famous European GDPR Regulation), cyber warfare (e.g. the Tallinn Manual 2.0). The definition or concept of cybersecurity used often varies according to the specific legal domain at hand [Kosseff, 2018, p. 985].

[5] E.g. the Council of Europe's Convention on Cybercrime. So far, 64 States have ratified this convention, 19 years after its official adoption [Pupillo, 2018, p. 4].

[6] The ITU Plenipotentiary Conference held in Guadalajara, Mexico, 2010, approved the definition. See Kshetri [2016, p. 3].

[7] See e.g. the United Nations Office on Drugs and Crime (UNODC) Global Programme on Cybercrime, ITU Global Cybersecurity Index, UN Digital Blue Helmets, and the work within the Group of Governmental Experts on Information and Telecommunications Developments in the Context of International Security ("UN GGE") (First Committee of the UN General Assembly).

[8] See e.g. the 2013 Cybersecurity Strategy, the establishment of ENISA (European Union Agency for Network and Information Security), the Cyber Defence Policy Framework (2014, updated in 2018), the development of cyber defence related projects under the Permanent Structured Cooperation (PESCO), the Joint Framework on Countering Hybrid Threats (2016), the Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016), and the 2017 Framework for a Joint Diplomatic Response to Malicious Cyber Activities ('EU Cyber Diplomatic Toolbox').

[9] In particular, one with supranational features [Schermers, Blokker, 2018, §60–61, 60–62].

[10] Calls have been made to regionalize cybersecurity regulation [Henriksen, 2019, pp. 5–7].

in the UN and the EU. First, on a more abstract level, the article will discuss whether international law can adequately regulate issues of cybersecurity: what impediments are encountered in regulating in the cyber domain? Vice versa, can the high-tech phenomenon of cybersecurity be embedded in international law? (II) The article surveys the work of the Group of Governmental Experts on Information and Telecommunications Developments in the Context of International Security (hereinafter: "UN GGE"), whereby the question arises whether its reports represent an emerging international *opinio juris*. (III) The problems associated with regulating cybersecurity at the UN level have led to calls for action at the regional level. In the EU, many policy initiatives in different subdomains of cybersecurity have seen the light of day. Two legislative measures stand out: the 2016 Directive on Network and Information Security (hereinafter: "NIS Directive") [EU, 2016] and the 2019 EU Cybersecurity Act (IV) [Ibid., 2018]. The analysis thereof will allow one to discern whether and which impediments of regulating cybersecurity at the international level are shared at the EU legislative level (V). We conclude with some reflections on the desirability of regulating cybersecurity at the UN and EU levels. Are the difficulties of regulating cybersecurity embedded in the distinct lawmaking processes of the UN or the EU, or are they inherent to the phenomenon of cyberspace? At what level is cybersecurity regulation the most efficient, well-developed and promising? (VI).

## Cybersecurity and International Law: Strange Bedfellows

### *Factors Explaining the Difficult Marriage Between Cybersecurity and International Lawmaking*

The difficult marriage between cybersecurity and international lawmaking can be explained by a number of factors [Tranter, 2007, p. 449].

#### *Fast and High-tech Cyber Revolution*

The digitization of the world is taking place at an unparalleled pace [Niemann, 2018, pp. 907–25]. It is expected that by the end of 2020 there will be more than 20 billion connected devices [Reuters Plus, 2018; Sandage et al., 2013, p. 1]. In contrast to how international lawmakers responded in a timely manner to certain developments in the twentieth century, such as the international law of the sea concept 'exclusive economic zone' (EEZ) [UN, 1982] and the protection of the seabed as 'common heritage of mankind' [UN, 1970], the cyber revolution is often said to be so fast and unpredictable that international lawmaking has difficulties catching up [Kittichaisaree, 2017, p. 336].

#### *Sovereignty, Territoriality, Fragmentation of Jurisdiction and Legal Attribution*

The core concept on which international law rests, State sovereignty, does not fit effortlessly with cyberspace [Vergne, Duran, 2014, pp. 126–139]. Although – thanks to the work of the UN GGE – there is agreement that the principle of State sovereignty applies in cyberspace [G20, 2015; Schmitt et al., 2017, Rule 1, p. 11; UN, 2013; 2015], no State can claim sovereignty over the entire cyberspace [Sandage et al., 2013, pp. 184; Schmitt et al., 2017, Rule 1.7]. The reason for this is that the many cyber infrastructures that make up cyberspace are located in different sovereign territories [Schmitt et al., 2017, Rule 1.7], and that in international law, territoriality allocates jurisdiction. Nonetheless, as Trachtman rightly observes, this fragmentation of jurisdiction should not be a reason to give up regulating cybersecurity altogether: after all, (cyber)conduct still occurs in a certain territory and effects are still felt in a certain territory

[Trachtman, 2013, p. 88]. Issues that transcend territorial jurisdiction are by no means new to international law (e.g. the law of the high seas, outer space, climate change). The challenge lies in the problem of legal attribution: it is often difficult to determine the identity or location of cyberattackers or their intermediaries [Kshetri, 2016, p. 7; Wheeler, Larsen, 2013, p. 1]. This is the true complicating factor according to Trachtman [Healey, 2012; Shackelford, Russell, Kuehn, 2016, p. 10; Trachtman, 2013, p. 88]: even when there are rules on cybersecurity in place, the legal attribution problem may weaken their effectiveness.[11]

### *Role of the Government versus the Private Sector*

A third factor that underlies the difficult relationship between cybersecurity and international law is the question of the (extent of the) regulatory role of the State versus that of the private sector in cyberspace [Groupe UMP, 2009]. Cyberspace is a domain in which industry and the private sector play a pivotal role. The private sector governs cyberspace in an informal manner, leaving less room for the formal legislator (the nation State) [Hoisington, 2017, p. 95]. The question then arises to what extent the State must or can impose legal obligations on the private sector while regulating cybersecurity. Vice versa, to what extent can cybersecurity regulation be effective if the private sector is not involved in its preparation and implementation? There are heated discussions about the role of the State as regulator in cyberspace. On the one hand, one can argue that the nation State has the obligation to enact legislation that regulates or restricts the private sector in its cyber activities. The argument here is that the State must uphold its legal obligations under international law, such as the protection of human rights, international peace and security, the customary 'no harm' principle [ICJ, Corfu Channel Case, 1949; Trail Smelter case (United States v. Canada (1938 and 1941),[12] the protection of critical infrastructures [EU NIS Directive, 2016, *infra* Section IV], and so on. According to some, these obligations can only be guaranteed in the cyber domain if rights and obligations are imposed on private actors [Kittichaisaree, 2017, pp. 335–52]. On the other hand, some question whether the role of the State within the cyberdomain can and should be that far-reaching. The main arguments in favour of a limited oversight function of the State are: (i) the private sector does not have sufficient incentives to duly cooperate with the State since this could jeopardize its commercial objectives [Teplinsky, 2013, pp. 225–322] (i.e. reputation damage, counterattacks by competitors using released technology); (ii) regulation will slow down innovation [Contreras et al., 2013, pp. 1115, 1119]; and (iii) the private sector prefers a private legal system as opposed to public criminal law [Wall, 2007, pp. 25–6]. An alternative solution would be that the governance of cyberspace be observed on the basis of (binding or non-binding) codes of conduct originating from industry itself.[13] The two aforementioned views should not be seen as mutually exclusive [Trachtman, 2013, p. 90]: whether and to what extent the State should have a regulatory role in cyberspace depends on the specific conduct one wishes to regulate. The

[11] Fidler [2015] talks about this problem in the context of treaties on cybercrime when applied to protect critical infrastructure from cyber threats.

[12] ICJ 9 April 1949, Corfu Channel Case (United Kingdom v. Albania), *I.C.J. Reports* 1949, p. 4; Reports on International Arbitral Awards, Trail Smelter case (United States v. Canada), 16 April 1938 and 11 March 1941, 3 *UNRIAA*, pp. 1905–82.

[13] An example of such an influential code of conduct is the "NIST" (National Institute of Standards and Technology Cybersecurity) framework. As its proponents argue, this document "harmonizes consensus standards and industry best practices to provide a flexible and cost-effective approach to enhancing cybersecurity that assists owners and operators of critical infrastructure in assessing and managing cyber risk, as the standard for due diligence." NIST *inter alia* collaborates with the United Kingdom, Japan, Korea, Estonia, Israel and Germany. However, it has been observed that a disadvantage of NIST is that it is less well suited to protect enterprises from sophisticated and targeted cyberattacks [Shackelford, Russell, Kuehn, 2016, p. 42].

"institutional choice may begin with determining whether the issue at stake is best taken on by the market, by private firms, by the State government, or by international law."[14] Interestingly, the European NIS Directive imposes obligations on certain entities in the private sector (*infra,* Section IV)[15], acknowledging that cyberspace is a domain in which cooperation between the State and the private sector is often necessary.

#### *Applying Existing Law versus Creating New Law*

Is it sufficient to apply existing international law to the cyber domain, or should new rules be created that are specifically designed to address this challenge? Hoisington points to three competing views: (i) cybersecurity is to be addressed by using existing rules and structures under international law; (ii) cyberspace is fundamentally unique and requires new legal rules and structures; and (iii) existing law can tackle the challenge of cybersecurity, but those elements that are incompatible with its uniqueness should be set aside [Hoisington, 2017, p. 87]. What has been done so far on the international plane largely reflects the first view: the UN GGE has declared that international law, including the UN Charter, applies to cyberspace (*infra*), whereas the Tallinn Manual 2.0 transposes fundamental principles of international law to cyberspace in general (notably Rules 1–24) and more specifically to cyberwarfare.

#### *Cyber Mania*

Cyber mania is another phenomenon that complicates the relationship between international law and cybersecurity [Kshetri, 2016, p. 2; von Heinegg, 2012, p. 5]. While developments in the field of cybersecurity law *sensu stricto* have been limited, a considerable amount of academic attention and policy interest has been devoted to the specific issue of 'cyberwarfare law'. According to O'Connell, the highly mediatized cyberattacks in Estonia (2007), the cyber incidents during the Russo-Georgian conflict (2008) and Stuxnet (2010) gave rise to this militarized image of cybersecurity law [O'Connell, 2012, p. 191]. The majority of cyber incidents indeed does not reach the threshold of 'armed attack' within the meaning of Article 51 of the UN Charter [ENISA, 2015]. In reality, cyber threats are more complex and diverse in nature and often target private companies [Second recital, Preamble of the NIS Directive; d'Elia, 2014, pp. 240–60].

#### ***Interim Conclusion***

Given these multiple challenges, it is perhaps less surprising that there currently exists no global convention in the field of cybersecurity *sensu stricto*. The UN initiative that comes closest is the work of the UN GGE. In the next section, we analyze the reports of the UN GGE and explore their legal relevance.

## The UN Group of Governmental Experts[16]

The issue of information security first featured on the UN agenda in 1998, when the Russian Federation submitted a draft resolution on the topic in the First Committee of the UNGA. The UNGA adopted it without a vote as Resolution 53/70 [UN, 1998]. Since 2004, the UN GGE has studied the threats posed by the use of ICTs in the context of international security and how

[14] Trachtman [2013], according to whom this choice reflects the "true meaning of subsidiarity."

[15] A careful reading of the NIS Directive makes it clear that ultimately, it are the Member States that must ensure that providers of essential and digital services comply with the obligations set out in articles 14 and 16 of the Directive (security and reporting requirements).

[16] This article is up-to-date until March 2020.

these threats should be addressed. Its work addresses issues of international law, in parallel to discussions on existing and emerging threats, norms, rules and principles, confidence building measures and capacity building [OEWG, 2020f]. The UN GGE reports of 2013 and 2015 are the most important and impactful ones. In its consensual report of 24 June 2013, the UN GGE established that international law, and in particular the UN Charter, applies in cyberspace just like in the physical space [UN, 2013, Para 19]. This includes the rules on State sovereignty and the principles resulting from the notion of sovereignty. For example, a State has jurisdiction over ICT infrastructure on its territory, and the State is responsible for international unlawful cyber acts that can be attributed to it [UN, 2013, Para 20; Schmitt et al., 2017, Rules 1–13]. In its consensual report of 2015, the UN GGE put forward the following principles of the UN Charter and international law as applicable in cyberspace to state behaviour: "sovereignty, sovereign equality, peaceful conflict resolution, the prohibition of the use of or threat of violence against the territorial integrity or political independence of a State, respect for human rights and fundamental freedoms and the principle of non-intervention in the internal affairs of other States" [UN 2015, Para. 28b]. This transposition to cyberspace of the fundamental principles of international law, which almost all constitute binding customary international law and/or have been confirmed by the International Court of Justice, is subject to a fairly broad consensus.[17] Several States, including certain 'cyber superpowers', had since confirmed the applicability of international law in cyberspace in their comments to the UN GGE reports and in their national cyber security strategies [République Française, 2018, paras 82, 85 and 87; Australian Government, 2016, paras 7, 28 and 40–41; Government of the Russian Federation, 2016, para 34; U.K. Government, 2016, para. 63]. This applicability was equally confirmed by the G20 in 2015 [G20, 2015, §26]. At that point in time, the UN GGE 2013 and 2015 reports could be seen as an indication of a growing consensus on the matter, and as evidence of the development of a certain *opinio juris,* which is one of the elements needed to eventually generate customary international law [Wouters et al., 2018, pp. 149–52].[18] Note that in the cybersecurity domain, State practice is largely classified and "partly contradictory" [Väljataga, 2018, pp. 4–5].

However, in June 2017, during the fifth meeting of the UN GGE, any meaningful development of *opinio juris* came to an abrupt end. Fundamental differences between the 25 members emerged, mainly on the issue of self-defence and on applying international humanitarian law to cyber conflicts. The Cuban delegation refused to recognize the explicit reference in the text to the applicability of the right to self-defence in cyberspace. According to the delegation, this would "legitimize an ICT war" [Soesanto, d'Incau, 2017]. The Cuban, Russian and Chinese delegations suggested the development of an entirely new set of international regulations and the creation of a UN General Assembly Working Group that would be open to all States, where 'transparency, exclusivity and participation are central to discussion and decision-making'. The U.S. interpreted this as undoing all earlier progress made within the UN GGE [Bowcott, 2017]. As seen above, the 2013 UN GGE report confirmed the applicability of the UN Charter to cyberspace, and with this *implicitly* article 51 UN Charter, which concerns the right to individual and collective self-defence of a State. The same goes for the 2015 UN GGE report.[19] The Cuban

[17] These fundamental principles are reiterated throughout the Tallinn Manual 2.0 as being 'black letter rules' applicable in cyberspace; Henriksen [2019, p. 4].

[18] See also UN [2018c, Draft Conclusion No 9 and Commentary]; Haggenmacher [1986, p. 5]; Bederman, [2010]; and Bradley [2016]. Note that the UN GGE is of limited membership, but the 2013 and 2015 rounds did include what are understood to be the most powerful cyber nations, such as the U.S., U.K., China and Russia.

[19] The UN GGE 2015 agreed on the applicability of the principles of international humanitarian law in the following terms: "The Group notes the established international legal principles, including, where appli-

argument was thus not so much legal as it was political. At the end of the 2017 session, no consensus report was adopted. By the end of 2018 the UN GGE was seemingly defunct [Bowcott, 2017; Henriksen, 2019, pp. 6–13; Soesanto, d'Incau, 2017].

In December 2018, though, agreement was found in the UNGA to establish two distinct processes in order to discuss the issue of security in the use of ICTs during the period of 2019–2021. With Resolution 73/27, sponsored notably by Russia [Ruhl et al., 2020], the UNGA established the Open-ended Working Group (hereinafter: "OEWG"), to the delight of the Cuban and Chinese delegations [UN, 2018a]. Eleven days later, the UNGA endorsed the commencement of the work of the sixth UN GGE, which is now called the 'UN GGE 2019–21 on advancing responsible State behavior in cyberspace in the context of international security' [Ibid., 2018b]. This resolution was sponsored by the U.S. It is worth noting that, whereas the OEWG is open to all interested UN Member States,[20] the UN GGE for the period of 2019–21 consists of 25 selected Member States: Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, Netherlands, Norway, Romania, Russian Federation, Singapore, South Africa, Switzerland, United Kingdom, United States, and Uruguay [Ruhl et al., 2020; UN, 2018b, Para. 3]. While the UN GGE 2019–21 addresses norms, rules and principles, confidence building measures and capacity building and how international law applies to cyberspace [Geneva Internet Platform, n. d.], the OEWG can further develop or change norms, rules and principles listed in Resolution 73/27, confidence building measures and capacity building, how international law applies to cyberspace, existing and potential threats, establishing regular institutional open-ended dialogue within UN and relevant international concepts for securing global IT systems [UN, 2018a, Para. 5]. It has pointedly been observed that "the GGE and OEWG's overlapping mandates suggest that they could operate as a sum greater than the parts – but it is important to recall that the OEWG is the product of a Russian proposal designed specifically to substitute for the U.S. call for another GGE" [Ruhl et al., 2020].[21]

---

cable, the principles of humanity, necessity, proportionality and distinction" [UN, 2015, Para. 28.d].

[20] Some see this as an attempt by Russia to include more countries which would support its interests in cyberspace. See Grigsby [2018], Iasiello [2019].

[21] These authors see a risk of competition or even conflict between the two processes, and contend that "the United States and its allies see the OEWG as a forum for new stakeholders to learn about and spread the extant GGE norms. Russia, in contrast, may prefer to revisit previous GGE reports under the OEWG and revise them to better align with its interests. And while the 2015 GGE agreed on the applicability of the principles of international humanitarian law, this position was not noted in the establishment of the OEWG." See in the same vein E. Iasiello [2019]: "The OEWG met in mid-September 2019 and some of the larger issues such as international humanitarian law that had previously prevented consensus surfaced again. While States like China and Russia have pushed back on international humanitarian law in the GGE, the OEWG meeting showed more States like Egypt for instance would be more inclined to back that position by placing less emphasis on its importance than other areas. More importantly, States that had not been able to express their opinions in the GGE now have a vehicle to accomplish that. States like Iran have been able to submit written statements highlighting their positions on issues. The larger OEWG may be the preferred avenue for States like China, Iran, and Russia that share the same philosophies with regards to cyberspace. Moreover, the opening of discussions to any UN Member State enables these governments to push for their preferred issues like cyber sovereignty (and by extension all that comes with it such as the controlling of potentially harmful information) by gaining the backing from other, smaller States, that might not otherwise have a say in the state-limited GGE. More authoritarian or closed countries may find themselves supporting the positions of their Chinese/Russian counterparts for the same reasons. Considering this, it comes as no surprise that Western countries like Australia, the United Kingdom, and the United States voted against OEWG's establishment."

The tentative programme of work (2019–2021) for the two processes looks as follows.

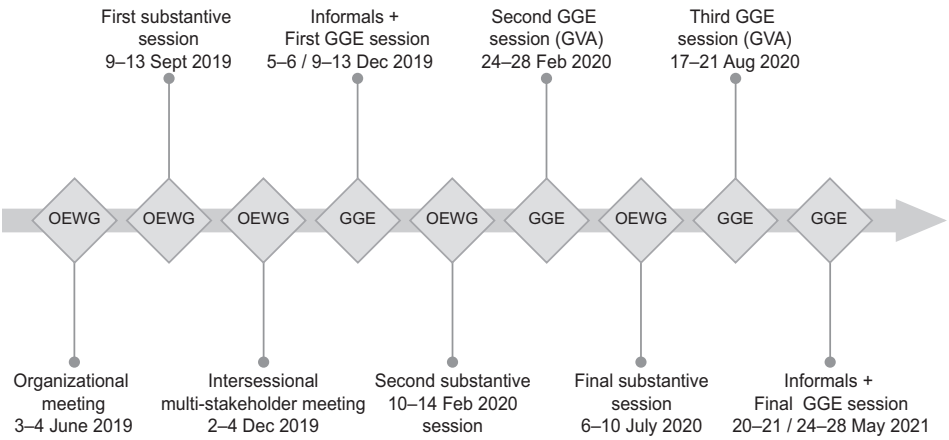


*Fig. 1.* Tentative GGE and OEWG "timeline" (2019–21)

*Source:* United Nations Office for Disarmament Affairs [n. d.].

Concerning the OEWG, the present article analyzed the publicly available documents of (i) the organizational session of 3–4 June 2019 [UN, 2019a; 2019b], (ii) the first substantive session of 9–13 September 2019 [UN 2019c; OEWG, 2019f], (iii) the informal multi-stakeholder meeting of 2–4 December 2019 [OEWG, 2019b; 2019c; 2019d; 2020a], and (iv) the second substantive session of 10–14 February 2020.[22] The analysis shows that the process is still very much in the stage of an exchange of views, with members discussing what the focus of the OEWG's work should be. Members e.g. expressed that 'the new (current) GGE and the OEWG should be mutually supportive and avoid contradictions' [OEWG, 2020b]. The same can be said after analysis of the publicly available documents of the informal and first GGE session in December 2019.[23] This makes sense, as the OEWG is due to report to the 75th session of the UNGA, which takes places in the second half of 2020 [UN Office for Disarmament Affairs, 2019]. The UN GGE is due to report to the 76th UNGA session in 2021 [UN, 2018b, Para. 3].

While – especially in light of the more recent developments – it cannot longer be upheld that the UN GGE 2013 and 2015 reports represent an indication of a growing *opinio juris* of the international community, they nevertheless constitute an important indication of the applicability of international law to cyberspace. It remains to be seen if and what progress the OEWG and GGE processes will bring about, and whether these will result in a reaffirmation of certain principles, which could contribute to a development of an international *opinio juris*, or whether the outcomes of these processes, because of their political divides, will directly or indirectly conflict with each other and thereby neutralize any emerging *opinio juris*. Henriksen professed that the 2017 deadlock within the UN GGE would lead to more regional initiatives between like-minded States, such as at the EU level.[24] This is what the article now turns to.

[22] Non-exhaustively, OEWG [2019e; 2020b; 2020c; 2020d; 2020e; 2020f; 2020g]. See also the working papers submitted by Member States and informal papers submitted by intergovernmental organizations at the UN Office for Disarmament website [n. d.]. See Kaspar and Kumar [2019].

[23] At the time of submission, no documents of the second GGE session (24–28 February 2020) were available.

[24] According to Henriksen, the "regionalization of cybersecurity regulation into legal sub-systems of varying normative depth is unfortunate, given the global nature of the Internet." At the same time, Henriksen ad-

## The EU 2016 NIS Directive and 2019 Cybersecurity Act

The EU has been vocal about its wish to play a leading role in cybersecurity [EU, 2018, Recital 15, Preamble]; EC, High Representative of the European Union for Foreign Affairs and Security Policy [2013, pp. 7, 11]; EC [2013a, p. 5; 2018, p. 1]; Westby, 2019; Fantin, 2019; Niebler, 2019.[25]

The NIS Directive is the EU's first ever horizontal and legally binding instrument on cybersecurity *sensu stricto*. It aims to protect critical infrastructure (essential service providers and digital service providers) from cyber incidents that have a that have an 'actual adverse effect' on the security of network and information systems [EU, 2016, Art. 4.7]. The European Parliament and the Council of the EU adopted the Directive on 6 July 2016, which had to be implemented by 9 May 2018 in the national legal orders of the EU's Member States. The primary objective of the NIS Directive is "to guarantee a high common level of network and IT security" [Ibid., Fourth Recital, Preamble]. One of the main reasons for its adoption was that some EU Member States did not have cybersecurity legislation in place, and even when they did, there were large divergences among Member States. The EU's legislature was worried because 'cyber incidents are increasing in size, frequency and complexity and can result in business inability to do their jobs, significant financial losses to the EU economy and a loss of welfare for society' [Ibid., Second Recital, Preamble].

The NIS Directive imposes various obligations upon Member States, including ensuring a minimum national capacity by designating NIS competent authorities, by setting up computer crisis teams and through national NIS strategies and cooperation plans.[26] Interestingly, the Directive also imposes obligations onto two categories of private sector entities, namely the providers of essential services and providers of digital services.[27] The Directive sets out the

---

mits that there are advantages to a more regional approach to cyber regulation, such as "avoiding time-consuming negotiations, the perspective of reaching agreement on complex issues rather than just on the low-hanging fruits," etc. See Henriksen [2019, p. 6]. In the wake of the 2017 UN GGE failure, US Homeland Security advisor Tim Bossart expressed that "it is now time to consider other approaches (...) and that the U.S. will work with smaller groups of like-minded partners." See The White House [2017].

[25] See also *supra* note 9.

[26] Each Member State must ensure a minimum national capacity by designating NIS competent authorities (art. 8 NIS Directive), by setting up computer crisis teams ('Computer Emergency Response Teams' – CERTs or 'Computer Security Incident Response Teams' – CSIRTs) (art. 9) and through national NIS strategies and cooperation plans (art. 7). National competent authorities must work together within a network (the Cooperation Group) that allows secure and effective coordination, including coordinated information exchange, and detection and response at EU level. Member States must exchange information and collaborate through this network to tackle NIS threats and incidents on the basis of the European NIS cooperation plan (Art. 11). One of the most important obligations for Member States is to identify the providers of essential services (Art. 5). A culture of risk management should be promoted (see recitals 4 and 44, Preamble NIS Directive) and the private and public sectors should cooperate and exchange information with each other. See EU [2016, Recital 35, Preamble], R. Roex [2016].

[27] The Directive focuses on two types of entities in the private sector (Articles 1, 4, 5, 14, 16): (i) providers of essential services and (ii) digital service providers. According to Article 5 (2) of the NIS Directive, providers of essential services are entities that 'provide services that are essential for the maintenance of critical social and / or economic activities, the provision of that service depending on network and information systems and in which in the event of an incident would have significant disruptive effects on the provision of that service'. In its Annex II, the NIS Directive specifies in a non-exhaustive way the sectors in which the Member States must search for the providers of essential services. These include the following sectors: banks, stock exchanges, transport and distribution of energy, air, rail and maritime transport, health, internet services and the government. Nuclear installations fall outside the scope of the Directive. See L. Lemmens [2018]. Digital service providers, the second private sector entity onto which the Directive imposes obligations, should be understood as online marketplaces, online search engines and cloud computer services. They are exhaustively listed in Annex III of the Directive. During the legislative process, it was decided that many of the other suggested digital services

following security and reporting requirements for providers of essential and digital services: (i) take appropriate technical and organizational measures to manage NIS risks; (ii) prepare and implement business continuity plans; (iii) notify the competent authority or CSIRT of an incident that has a significant impact on the continuity of the services they provide. What exactly constitutes a cyber incident with a 'significant impact' is thus quintessential to the implementation of the Directive, yet the meaning of this term is unclear at this stage[28] and it remains to be seen how this will be applied in practice[29].

Secondly, one should point to the EU's Cybersecurity Act, laid down in Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the EU Agency for Cybersecurity) and on information and communications technology cybersecurity certification [EU, 2018]. The Regulation entered into force on 27 June 2019. The legal basis of the Regulation is art. 114 TFEU, which aims to further the objective of a properly functioning internal market as laid down in article 26 TFEU [EU, 2012; Mitrakas, 2018, p. 411]. The Cybersecurity Act has come about due to several factors, in particular the EU's ambition to be a leader in the world's cybersecurity market as well as its realization that the current framework is unable to quickly respond to certain threats, as evidenced by recent cyberattacks [Fantin, 2019]. Substantively, the Act introduces a pan-European cybersecurity certification scheme.[30] This should remedy the risk of market fragmentation[31] and should allow the EU to compete in the global cybersecurity arena [Mitrakas, 2018, p. 411]. The certificates will attest that a product or service meets certain evaluation criteria and provides for a warranted level of cybersecurity assurance [Ibid., p. 413].[32] An important obligation for Member States under the Act is to designate one or more national cybersecurity certification authorities in their territory or, with the agreement of another Member State, to designate one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State [EU, 2018, Art. 58.1]. In addition, the Regulation bestows upon ENISA, the European Union Agency for Cybersecurity, a permanent mandate and strengthens its role by providing it with more resources and by attributing further tasks.[33] Article 6 of the Cybersecurity Act stipulates that ENISA will assist Member States in their capacity building (e.g. in establishing and implementing vulnerability disclosure policies [Ibid., Art. 6.1(b)] and in developing national CSIRTs, making a direct link with the NIS Directive [Ibid., Art. 6.1(d)], although but note that the measures referred to in Art. 6 reflect best efforts obligations on the part of Member States.

---

were not critical enough. See Roex [2016]. Under the NIS Directive, Member States are not required to identify digital service providers, allowing for a 'catch-all approach', see D. Markopoulou, V. Papakonstantinou and P. de Hert [2019, p. 4].

[28] Some guiding elements to determine what a significant effect is, are mentioned in art. 14.4 and 16.4 of the NIS Directive.

[29] A careful reading of the Directive makes it clear that, ultimately, it are the Member States that must ensure that providers of essential and digital services meet the security and reporting requirements of Articles 14 and 16.

[30] With a view to creating a digital single market for ICT products, ICT services and ICT processes, as the Act in art. 46.1 itself posits. See the security objectives of European cybersecurity certification schemes in art. 51 of the Act.

[31] E.g. France had already developed its own security certification scheme; 'Certification Sécuritaire de Premier Niveau' [Mitrakas, 2018, p. 412].

[32] Note that the schemes are currently voluntary. After a four-year period, the European Commission will be in a position to impose certain mandatory requirements if it sees fit [Fantin, 2019].

[33] Fantin has said that with this, the EU now considers ENISA an important actor to turn to for advice on potential 5G procurement and rollout [Fantin, 2019].

## Cybersecurity and EU Law: Irreconcilable?

Above, the article identified five factors that explain the difficult relationship between international lawmaking and cybersecurity. It will now be scrutinized whether (some of) these difficulties are shared at the EU legislative level.

### *Fast and High-tech Cyber Revolution*

The fact that the cyber revolution is a fast and high-tech one is inherent to the concept itself, and thus present at both the UN and the EU level. Evidently, the regional and limited membership of the EU, the like-mindedness of its membership, the absence of great cyber powers from the negotiating table as well as the established legal instruments, competences and supranational features of the EU explain why the EU has somewhat less trouble in catching up with the speed of the cyber revolution.

### *Sovereignty, Territoriality, Fragmentation of Jurisdiction and Legal Attribution*

The fact that cyberspace has no territorial limits is inherent to the concept itself and thus present at both the UN and the EU level. Concerning the NIS Directive, seeing how a country's critical infrastructure is most often located within its territory (e.g. drink water systems, hospitals, railways) [EU, 2016, Annex II] and thus within its territorial jurisdiction, EU governments can in general protect it without necessarily relying on international law [Fidler, 2015, pp. 9–10], thereby being less subject to the problem of fragmented jurisdiction. This is similar for the Cybersecurity Act, of which Article 58 stipulates that "each Member State shall designate one or more national cybersecurity certification authorities in its territory or, with the agreement of another Member State, shall designate one or more national cybersecurity certification authorities established in that other Member State to be responsible for the supervisory tasks in the designating Member State. National cybersecurity certification authorities shall: (a) supervise and enforce rules (...) for the monitoring of the compliance of ICT products, ICT services and ICT processes with the requirements of the European cybersecurity certificates that have been issued in their respective territories (...); monitor compliance with and enforce the obligations of the manufacturers or providers of ICT products, ICT services or ICT processes that are established in their respective territories (...)" [EU, 2018, Art. 58.1, 58.7(a), (b)]. Nevertheless, as seen, the more fundamental issue here lies in the more fundamental issue here lies in the legal attribution problem. This problem is also present at the EU level, and may equally weaken the effectiveness of its cybersecurity rules.

### *Role of the Government versus the Private Sector*

The fact that cyberspace is informally governed by the private sector poses a problem to regulators at both the EU and UN levels. In the NIS Directive, the EU legislature acknowledges the importance of imposing not only obligations on the Member States' authorities, but also on the private sector, notably the providers of essential services mentioned in Annex II of the Directive and the providers of digital services mentioned in Annex III of the Directive. The EU has the experience, legal tools, and internal market competences to do so. While the NIS Directive and the Cybersecurity Act allow Member States to lay down the rules for penalties in case of infringement [Ibid., 2016, Art. 21; 2018, Art. 65], this is no guarantee that the private sector has a sufficient incentive to duly cooperate with the State at the possible expense of its commercial objectives, nor that the regulations will not slow down innovation. It also remains to be seen how EU Member States will interpret a 'cyber incident

with a significant impact on the continuity of essential and digital services,' and whether they can effectively ensure that operators of essential services and digital services notify the competent authority or CSIRT of such incidents [EU, 2018, Art. 14.3, 16.3], without which a lot of the measures of the NIS Directive are rendered meaningless of the NIS Directive are meaningless.

### *Applying Existing Law versus Creating New Law*

The NIS Directive and the Cybersecurity Act are examples of new rules being created after cybersecurity emerged as a policy problem. The political momentum in the Union, an organization with far-reaching legislative powers, to take a geopolitical direction on the matter plays a significant role.

### *Cyber Mania*

Cyber mania posing less of a problem at EU than at UN level requires little further explanation. The EU does not have the same mandate nor membership in the field of international peace and security as does the UN; neither does the UN have the same mandate in the field of economic policy and internal market and competition as does the EU.

### *Legal Binding Force*

As any EU regulation, the Cybersecurity Act has been binding in its entirety across the EU ever since it entered into effect on 27 June 2019.[34] As any EU directive, the NIS Directive is legally binding as well.[35] Portraying the legally binding force of these measures as a success to the detriment of UN efforts on cybersecurity would, however, be misleading. It is not particularly difficult to explain why consensus on legally binding measures could be found on this topic within the EU. Apart from the evident reasons (legal tools available to the EU, competences, supranational features, like-minded group argument), the NIS Directive introduces measures to protect critical infrastructures, a concept well defined in EU law [EC, 2005, Annex 1, p. 20; EU, 2008, Art. 2(a)] and at the forefront of international concerns in cybersecurity discussions [European Commission, 2005; 2009; 2013b; Melzer, 2011; UN, 2004]. The NIS Directive and the Cybersecurity Act were developed in the framework of the EU's longstanding and well-established competence to legislate on the internal market.

For now, it seems that almost all factors which hamper international cybersecurity regulation are inherent to the cybersecurity concept. They are therefore present both at the global and regional level and complicate the normative processes of the UN and the EU, however distinct they are. From this it should not be derived that regulation of cybersecurity *sensu stricto* should exclusively be done at either the UN or the EU level. The EU itself stated very recently, in the margins of the second substantive session of the OEWG, that "[t]he EU and its Member States support further engagement with key international and regional partners and organizations as well as with civil society, academia and the private sector in this field *with the aim of avoiding duplication of effort* [red.], and *looking for opportunities for synergies and burden-sharing* [red.], in order to support coordination and coherence in our collective efforts" [EU, 2019, authors' emphasis].

[34] Art 288, Para. 2 TFEU: "A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States" [EU, 2012].

[35] See Art 288, Para. 3 TFEU: "A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods" [EU, 2012].

## Concluding Remarks

This article identified five factors explaining the slow emergence of a global governance framework for cybersecurity, underlying the difficult relationship between cybersecurity and international law. They include the high speed at which global digitization is taking place as well as the nature of cyber operations; the fragmented jurisdiction and legal attribution problem; the question whether and to what extent the State and/or the private sector should have a regulatory role in cyberspace; whether transposing existing international law to the new technological context suffices; and the phenomenon of 'cyber mania'.

The EU has managed to issue two legally binding acts on cybersecurity *sensu stricto.* It remains to be seen how and if the obligations in these acts are effectively implemented and complied with.[36] The legally binding force of the NIS Directive and Cybersecurity Act should not make one conclude that the UN's work on cybersecurity has been a failure. Indeed, as is well-known in international law, soft law can be more effective than one might assume [cf. Boyle, 1999, pp. 901–12; Pauwelyn, Wessel, Wouters, 2012, pp. 159–60; Reisman, 1988, pp. 373–7; Virally, 1983, pp. 166–327; Wouters et al., 2018, pp. 165–7]. The work of the UN GGE between 2004 and 2017 made clear that international law applies to State behavior in cyberspace and brought together those States that actually are most engaged in cyber operations (China, Russia, U.S.). Yet, the UN GGE ran into troubles in going from the *whether* to the *how* [cf. Henriksen, 2019, p. 2]. At this moment in time, the UN faces a real risk that the splitting up into two processes – with the current GGE and the OEWG – will make overall agreement less likely, and drift further away from an international *opinio juris*. Regulating cybersecurity is stalled more because of politics than because of law at the UN level, whereas the current geopolitical momentum at the EU for regulation is high. In any case, advocating to exclusively regulate cybersecurity *sensu stricto* at either the UN or the EU level is a false dichotomy. Rather, synergies and cooperation should be sought. It would be highly regrettable if this proved impossible due to political rivalries and contestation.

## References

African Union. (2014) *Convention on Cyber Security and Personal Data Protection of 27 June 2014*, entry into force on 3 June 2019. Available at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf (accessed 9 March 2020).

Albrecht D. (2018) Chinese Cybersecurity Law Compared to EU-NIS-Directive and German IT-Security Act. *Computer Law Review International*, vol. 19, no 1, pp. 1–6. Available at: https://doi.org/10.9785/cri-2018-190102.

Australian Government. (2016) *Australia's Cyber Security Strategy: Enabling Innovation, Growth and Prosperity*. Department of Home Affairs. Available at: https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf (accessed 9 March 2020).

Bederman D. (2010) *Custom as a Source of Law*. Cambridge: Cambridge University Press.

Bowcott O. (2017) Dispute Along Cold War Lines Led to Collapse of UN Cyberwarfare Talks. *The Guardian*, 23 August. Available at: https://www.theguardian.com/world/2017/aug/23/un-cyberwarfare-negotiations-collapsed-in-june-it-emerges (last accessed 7 March 2020).

[36] Not only for the legal reasons we identified in this article, but also out of potential policy weaknesses. See e.g. C. Ducuing [2019, p. 23–4], D. Albrecht [2018, pp. 1–6] and to a lesser extent D. Markopoulou, V. Papakonstantinou and P. de Hert [2019, pp. 1–11]. See also Mitrakas [2018, pp. 411–14], Pupillo [2018, pp. 1–6] and Fantin [2019].

Boyle E. (1999) Some Reflections on the Relationship of Treaties and Soft Law. *International and Comparative Law Quarterly*, vol. 48, no 4, pp. 901–13. Available at: https://doi.org/10.1017/S0020589300063739.

Bradley C. (ed.) (2016) *Custom's Future: International Law in a Changing World*. Cambridge: Cambridge University Press.

Contreras J., de Nardis L., Teplinsky M. (2013) Mapping Today's Cybersecurity Landscape. *American University Law Review*, vol. 62, no 5, pp. 1113–30. Available at: https://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1883&context=aulr (accessed 21 April 2020).

Council of Europe. (2001) Budapest Convention on Cybercrime. *ETS*, no 185, open for signature 23 November 2001, entry into force 1 July 2004. Available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561 (accessed 20 April 2020).

d'Elia D. (2014) La guerre économique à l'ère du cyberspace [Economic Warfare in the Cyberspace Era]. *Hérodote*, vol. 152/153, no 1, pp. 240–60. Available at: https://www.cairn.info/revue-herodote-2014-1-page-240.htm (accessed 21 April 2020).

Ducuing C. (2019) *On the Edge of the NIS Directive: The Proposed CITS Delegated Regulation, Friend or Foe?* CiTiP Working Paper, KU Leuven Centre for IT & IP Law. Available at: https://dx.doi.org/10.2139/ssrn.3486978.

European Commission (EC). (2005) *Green Paper on a European Programme for Critical Infrastructure Protection*. COM/2005/0576 final/. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52005DC0576 (accessed 21 April 2020).

European Commission (EC). (2009) *Protecting Europe From Large-Scale Cyber Attacks and Disruptions: Improving Preparedness, Security and Resilience. Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection*. COM(2009) 149 final. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF (accessed 21 April 2020).

European Commission (EC). (2013a) *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 2013/0027 (COD). Available at: https://ec.europa.eu/transparency/regdoc/rep/1/2013/EN/1-2013-48-EN-F1-1.Pdf (accessed 21 April 2020).

European Commission (EC). (2013b) *Making European Critical Infrastructures More Secure. Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection*. SWD(2013) 318 final. Available at: https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf (accessed 21 April 2020).

European Commission (EC). (2018) *Building Strong Cybersecurity in Europe*. State of the Union, 12 September. Available at: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_en.pdf (accessed 21 April 2020).

European Commission (EC), High Representative of the European Union for Foreign Affairs and Security Policy. (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions.* Brussels, JOIN(2013) 1 final. Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf (accessed 21 April 2020).

European Court of Auditors. (2019) *Challenges to Effective EU Cybersecurity Policy*. Briefing Paper, March. Available at: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf (accessed 20 April 2020).

European Union (EU). (2008) 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. *Official Journal of the European Union*, L 345/75, vol. 51, pp. 75–82. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2008.345.01.0075.01.ENG&toc=OJ:L:2008:345:TOC (accessed 21 April 2020).

European Union (EU). (2012) Consolidated Version of the Treaty on the Functioning of the European Union. *Official Journal of the European Union* C 326, vol. 55, pp. 47–200. Available at: https://eur-lex.europa.eu/

legal-content/EN/TXT/?uri=uriserv:OJ.C_.2012.326.01.0001.01.ENG&toc=OJ:C:2012:326:TOC#C_2012326EN.01004701 (accessed 21 April 2020).

European Union (EU). (2016) Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union (NIS Directive). *Official Journal of the European Union*, L 194/1. Available at: http://data.europa.eu/eli/dir/2016/1148/oj (accessed 20 April 2020).

European Union (EU). (2018) Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act). *Official Journal of the European Union*, L 151/1. Available at: http://data.europa.eu/eli/reg/2019/881/oj (accessed 22 April 2020).

European Union (EU). (2019) *EU Non-Paper on Capacity Building to Advance Peace and Stability in Cyberspace, for the Work of the Open-Ended Working Group on "Developments in the Field of Information and Telecommunications in the Context of International Security,"* Submitted to the Second Substantive Session of the OEWG (10–14 February 2020). Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/eu-non-paper-submission-oewg-2019.pdf (accessed 8 March 2020).

European Union Agency for Cybersecurity (ENISA). (2015) *Annual Incident Reports 2015*. Available at: www.enisa.europa.eu/publications/annual-incident-reports-2015 (accessed 7 March 2020).

Fantin S. (2019) *Weighting the EU Cybersecurity Act: Progress or Missed Opportunity? CiTiP Blog.* KU Leuven Centre for IT & IP Law, 19 March. Available at https://www.law.kuleuven.be/citip/blog/weighting-the-eu-cybersecurity-act-progress-or-missed-opportunity/ (accessed 6 March 2020).

Fidler D. (2015) Wither the Web? International Law, Cybersecurity and Critical Infrastructure Protection. *Georgetown Journal of International Affairs*, vol. 8, pp. 8–20. Available at: https://www.repository.law.indiana.edu/facpub/2452 (accessed 23 April 2020).

Futter A. (2018) Cyber Semantics: Why We Should Retire the Latest Buzzword in Security Studies. *Journal of Cyber Policy*, vol. 3, no 2, pp. 201–16. Available at: https://doi.org/10.1080/23738871.2018.1514417.

Geneva Internet Platform, Digital Watch Observatory. (n. d.) *UN GGE and OEWG*. Available at: https://dig.watch/processes/un-gge#view-7541-3 (accessed 7 March 2020).

U.K. Government. (2016) *National Cyber Security Strategy 2016–2021.* Available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 (accessed 9 March 2020).

Government of the Russian Federation. (2016) *Doctrine of Information Security of the Russian Federation. Ministry of Foreign Affairs of the Russian Federation,* 5 December. Available at: http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163 (accessed 9 March 2020).

Grigsby A. (2018) *The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased*. Net Politics Blog, 15 November. Council on Foreign Relations. Available at: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased (accessed 11 March 2020).

Group of 20 (G20). (2015) *G20 Leaders' Communiqué.* Antalya, 15–16 November. Available at: http://www.g20.utoronto.ca/2015/151116-draft-communique.pdf (accessed 21 April 2020).

Groupe UMP Assemblée nationale. (2009) *Le législateur et les questions de société: quelle méthode pour quels choix? Rapport d'étape du groupe de travail animé par Hervé Mariton, député de la Drôme à la demande de Jean-François Copé* [The Legislator and Questions for Society: Which Method for Which Choices? Progress Report for the Working Group Led by Hervé Mariton, Member of the Drôme at the Request of Jean-François Copé]. 12 May. Available at: https://www.unaf.fr/IMG/pdf/rapport_d_etape_mai_2009.pdf (accessed 6 March 2020).

Haggenmacher P. (1986) La doctrine des deux éléments du droit coutumier dans la pratique de la Cour Internationale [The Doctrine of the Two Elements of Cusstomary Law in the Practice of the International Court]. *Révue générale de droit international public*, vol. 90.

Harrison Dinniss A. (2018) The Threat of Cyber Terrorism and What International Law Should (Try To) Do About It. *Georgetown Journal of International Affairs*, vol. 19, pp. 43–50. Available at: https://doi.org/10.1353/gia.2018.0006.

Healey J. (2012) *Beyond Attribution: Seeking National Responsibility for Cyberattacks*. Issue Brief, Atlantic Council. Available at: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/ (accessed 9 March 2020).

Henriksen A. (2019) The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity*, vol. 5, no 1. Available at: https://doi.org/10.1093/cybsec/tyy009.

Hoisington M. (2017) Regulating Cyber Operations Through International Law: In, Out or Against the Box? *Ethics and Policies for Cyber Operations* (M. Taddeo, L. Glorioso (eds)). Oxford: Springer International.

Iasiello E. (2019) OEWG or GGE: Which Has the Best Shot of Succeeding? *Technative*, 5 December. Available at: https://www.technative.io/oewg-or-gge-which-has-the-best-shot-of-succeeding/ (accessed 22 April 2020).

International Telecommunications Union (ITU). (2008) *Overview of Cybersecurity, Recommendation ITU–T X.1205*. Available at: https://www.itu.int/rec/T-REC-X.1205-200804-I (accessed 22 April 2020).

Ivanov E. (2015) Combating Cyberterrorism Under International Law. *Baltic Yearbook of International Law Online*, vol. 14, no 1, pp. 55–69. Available at: https://doi.org/10.1163/22115897-90000120.

Kaspar L., Kumar S. (2019) Cyber Norms in NYC: Take-Aways From the OEWG Meeting and UNIDIR Cyber Stability Conference. *Global Partners Digital*, 12 June. Available at: https://www.gp-digital.org/cyber-norms-in-nyc-takeaways-from-the-oewg-meeting-and-unidir-cyber-stability-conference/ (accessed 21 April 2020).

Kittichaisaree K. (2017) Future Prospects of Public International Law of Cyberspace. *Public International Law of Cyberspace* (K. Kittichaisaree (ed.)). Switzerland: Springer International.

Kosseff J. (2018) Defining Cybersecurity Law. *Iowa Law Review*, vol. 103, no 3. Available at: https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/ (accessed 20 April 2020).

Kshetri N. (2016) Global Cybersecurity: Key Issues and Concepts. *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies* (N. Kshetri (ed.)). Springer International Publishing.

Lemmens L. (2018) *België werkt aan omzetting NIS-richtlijn voor uniforme beveiliging netwerk- en informatiesystemen* [*Belgium is Working on the Transposition of the NIS Directive for Uniform Security of Network and Information Systems*]. Wolters Kluwer Online, 22 November. Available at: https://polinfo.kluwer.be/newsview.aspx?contentdomains=POLINFO&id=VS300653460&lang=nl (accessed 21 April 2020) (in Dutch).

Schmitt M. et al. (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Markopoulou D., Papakonstantinou V., de Hert P. (2019) The New EU Cybersecurity Framework: The NIS Directive, ENISA's Role and the General Data Protection Regulation. *Computer Law & Security Review*, vol. 35, no 6, 1–11. Available at: https://doi.org/10.1016/j.clsr.2019.06.007.

Melzer N. (2011) *Cyberwarfare and International Law*. UNIDIR Resources, UN Institute for Disarmament Research. Available at: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf (accessed 9 March 2020).

Mitrakas A. (2018) The Emerging EU Framework on Cybersecurity Certification. *Datenschutz und Datensicherheit*, vol. 42, pp. 411–4. Available at: https://doi.org/10.1007/s11623-018-0969-2.

N. Kshetri (2009) Positive Externality, Increasing Returns and the Rise in Cybercrimes. *Communications of the ACM*, vol. 52, no 12. Available at: https://doi.org/10.1145/1610252.1610288.

Niebler A. (2019) Cybersecurity Act: New Momentum for Europe. *The European Files,* 25 March. Available at: https://www.europeanfiles.eu/industry/cybersecurity-act-new-momentum-for-europe (accessed 21 April 2020).

Niemann K. (2018) Unternehmensarchitektur und Digitalisierung: Eine Disziplin im Wandel [Enterprise Architecture and Digitalization: A Discipline in Change]. *HMD Praxis der Wirtschaftsinformatik*, vol. 55, no 5, pp. 907–27. Available at: https://link.springer.com/article/10.1365/s40702-018-00441-1 (accessed 21 April 2020).

Nye J. (2016/17) Deterrence and Dissuasion in Cyberspace. *International Security*, vol. 41, no 3, pp. 44–71. Available at: https://doi.org/10.1162/ISEC_a_00266.

O'Connell M. (2012) Cyber Security Without Cyber War. *Journal of Conflict & Security Law*, vol. 17, no 2, pp. 187–209. Available at: https://www.jstor.org/stable/26296226.

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2019a) *Updated List of Experts for the Presentations on the Six areas Outlined in Paragraph 5 (a)–(f) of the Provisional Agenda of the OEWG (A/AC.290/2019.1) as of 28 August 2019.* Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/280819-Updated-list-of-experts-first-substantive-session-OEWG-on-developments-in-the-field-of-information-and-telecommunications.pdf (accessed 9 March 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2019b) *Chair's Letter to the Member States for the Intersessional Meeting.* 1 November. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/oewg-chair-letter-to-member-states-for-intersessiona-meeting.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2019c) *Chair's Letter to the Participants of the OEWG Informal Intersessional Consultative Meeting.* 26 November. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/chairs-letter-to-participants-of-oewg-meeting-26-11-19.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2019d) *Calendar of Side Events.* Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/oewg-side-events-calendar.pdf (access 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2019e) *Chair's Letter to Member States on the Second Substantive Session*. 31 December. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-letter.pdf (access 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2019f) *Chair's Letter to Member States on the First Substantive Session*. 21 August. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/08/210819-OEWG-Chairs-letter-to-the-member-states-for-the-first-substantial-session.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2020a) *Chair's Letter on the Summary Report of the Informal Intersessional Consultative Meeting from 2–4 December 2019.* 28 January. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf (accessed 10 March 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2020b) *Chair's Working Paper for the Second Substantive Session in View of the Second Substantive Session (10–14 February 2020)*. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-working-paper-second-substantive-session.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2020c) *Draft Programme of Work*. Second Substantive Session – New York, 10–14 February 2020. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-draft-pow-second-substantive-session.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2020d) *Tentative Structure of the Substantive Component of the Report.* Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/191231-oeeg-chair-tentative-draft-structure-of-report-substantive-component.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2020e) *An Initial Overview of the UN System Actors, Processes and Activities on ICT-Related Issues of Interest to the OEWG, by Theme.* Background Paper. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2020f) *International Law in the Consensus Reports of the United Nations*

*Groups of Governmental Experts.* Background Paper. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-international-law-in-the-gges.pdf (accessed 22 April 2020).

Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). (2020g) *"Regular Institutional Dialogue" in the Consensus Reports of the United Nations Groups of Governmental Experts and the Mandate of the OEWG.* Background Paper. Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-regular-institutional-dialogue.pdf (accessed 22 April 2020).

Orji U.J. (2018) The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability. *Masaryk University Journal of Law and Technology*, vol. 12, no 2, pp. 91–129. Available at: https://doi.org/10.5817/MUJLT2018-2-1.

Pauwelyn J., Wessel R., Wouters J. (eds) (2012) *Informal International Lawmaking*. Oxford: Oxford University Press.

Pupillo L. (2018) EU Cybersecurity and the Paradox of Progress. *CEPS Policy Insights*, no 2018/06, Centre for European Policy Studies. Available at: https://www.ceps.eu/ceps-publications/eu-cybersecurity-and-paradox-progress/ (accessed 20 April 2020).

Reisman M. (1988) Remarks in Panel: A Hard Look at Soft Law. *Proceedings of the American Society of International Law*, vol. 82, pp. 373–7. Available at: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1747&context=fss_papers (accessed 21 April 2020).

République Français. (2018) *Revue stratégique de cyberdéfense* [*Cyber Defence Strategic Review*]. Secrétariat Général de la Défense et de la Sécurité Nationale, 12 February. Available at http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/ (accessed 9 March 2020).

Reuters Plus. (2018) *The Internet of Things Era: 6 Ways to Stay Safe*. 7 June. Available at: https://www.reuters.com/article/idUSWAOA6XIH2J6Z1858 (accessed 10 March 2020).

Roex R. (2016) EU keurt eerste algemene cybersecurity-wet goed [EU Adopts First General Cybersecurity Law]. *Wolters Kluwer Online*, 16 August 2016. Available at: https://legalworld.wolterskluwer.be/nl/nieuws/domein/strafrecht/eu-keurt-eerste-algemene-cybersecurity-wet-goed/ (accessed 21 April 2020) (in Dutch).

Ruhl C., Hollis D., Hoffman W., Maurer T. (2020) *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads*. Paper no 26, Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110 (accessed 22 April 2020).

Sandage J. et al. (2013) *Comprehensive Study on Cybercrime. United Nations Office on Drugs and Crime*. Available at: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 21 April 2020).

Schatz D., Bashroush R., Wall J. (2017) Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and* Law, vol. 12, no 2, pp. 53–74. Available at: https://doi.org/10.15394/jdfsl.2017.1476.

Schermers H., Blokker N. (2018) *International Institutional Law*. Amsterdam: Brill Nijhoff.

Shackelford S., Russell J., Kuehn A. (2016) Unpacking the International Law on Cybersecurity Due Diligence: Lessons From the Public and Private Sectors. *Chicago Journal of International Law*, vol. 17, no 1. Available at: https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1700&context=cjil (accessed 21 April 2020).

Soesanto S., d'Incau F. (2017) The UN GGE is Dead: Time to Fall Forward. Commentary, 15 August. *European Council on Foreign Relations*. Available at: https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance (accessed 22 April 2020).

Teplinsky M. (2013) Fiddling on the Roof: Recent Developments in Cybersecurity. *American University Business Law Review*, vol. 2, no 2, pp. 225–322. Available at: https://pdfs.semanticscholar.org/bf5d/e28421900aa225e054fd92e5f0a5bf9e03a0.pdf (accessed 21 April 2020).

The White House. (2017) *Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017*. TelAviv, 26 June. Available at: https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/ (accessed 10 March 2020).

Trachtman J. (2013) Cyberspace and Cybersecurity. *The Future of International Law: Global Government* (J. Trachtman (ed.)). Cambridge: Cambridge University Press.

Tranter K. (2007) Nomology, Ontology, and Phenomenology of Law and Technology. *Minnesota Journal of Law Science & Technology*, vol. 8, no 2, pp. 449–74. Available at: https://scholarship.law.umn.edu/mjlst/vol8/iss2/7 (accessed 21 April 2020).

United Nations (UN). (1970) *Declaration of Principles That Control the Sea-Bed and Ocean Floor, and the Subsoil Thereof, Beyond the Limits of National Jurisdiction. General Assembly Resolution A/RES/2749 (XXV)*. Available at: https://digitallibrary.un.org/record/201718?ln=en (accessed 21 April 2020).

United Nations (UN). (1982) Convention on the Law of the Sea. Concluded at Montego Bay on 10 December 1982, entry into force on 16 November 1994. *United Nations Treaty Series*, vol. 1833, I-31363. Available at: https://treaties.un.org/doc/Publication/UNTS/Volume%201833/volume-1833-A-31363-English.pdf (accessed 22 April 2020).

United Nations (UN). (1998) *Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Resolution A/RES/53/70.* Available at: https://undocs.org/A/RES/53/70 (accessed 21 April 2020).

United Nations (UN). (2004) *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures. General Assembly Resolution A/RES/58/199.* Available at: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_58_199.pdf (accessed 21 April 2020).

United Nations (UN). (2013) *Report of Group of Governmental Experts on Information and Telecommunications Developments in the Context of International Security. General Assembly Document A/68/98.* Available at: https://undocs.org/A/68/98 (accessed 21 April 2020).

United Nations (UN). (2015) *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/70/174.* Available at: https://undocs.org/A/70/174 (accessed 21 April 2020).

United Nations (UN). (2018a) *Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Resolution A/RES/73/27.* Available at: https://undocs.org/A/RES/73/27 (accessed 22 April 2020).

United Nations (UN). (2018b) *Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. General Assembly Resolution A/RES/73/266.* Available at: https://undocs.org/A/RES/73/266 (accessed 22 April 2020).

United Nations (UN). (2018c) *Draft Conclusions on Identification of Customary International Law, With Commentaries.* Available at: https://legal.un.org/ilc/texts/instruments/english/commentaries/1_13_2018.pdf (accessed 29 May 2020).

United Nations (UN). (2019a) *Provisional Agenda. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/AC.290/2019/1.* Available at: https://undocs.org/A/AC.290/2019/1 (accessed 22 April 2020).

United Nations (UN). (2019b) *Note by the Secretariat: Organization of the Work of the Open-Ended Working Group. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/AC.290/2019/ORG/CRP.1.* Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/07/sec-note-oewg-crp.pdf (accessed 22 April 2020).

United Nations (UN). (2019c) *Note by the Secretariat: Organization of Work of the First Substantive Session. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. General Assembly Document A/AC.290/2019/2.* Available at: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/08/A-AC.290-2019-2.pdf (accessed 22 April 2020).

United Nations (UN) (2020). (2020h) *Draft Organization of Work of the Second Substantive Session. Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). General Assembly Document A/AC.290/2020/1.* Available at: https://undocs.org/en/A/AC.290/2020/1 (accessed 22 April 2020).

United Nations (UN) Office for Disarmament Affairs. (n. d.) *Open-Ended Working Group.* Available at: https://www.un.org/disarmament/open-ended-working-group/ (accessed 10 March 2020).

United Nations (UN) Office for Disarmament Affairs. (2019) *Intergovernmental Processes on the Use of Information and Telecommunications in the Context of International Security 2019–2021.* Fact Sheet. Available at: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/03/2019+03+26+-+Fact+Sheet+Cyber+-+OEWG+and+GGE+processes+-+2.pdf (accessed 8 March 2020).

Väljataga A. (2018) *Tracing Opinio Juris in National Cyber Security Strategy Documents. NATO Cooperative Cyber Defence Centre of Excellence Paper.* Available at: https://ccdcoe.org/library/publications/tracing-opinio-juris-in-national-cyber-security-strategy-documents/ (accessed 22 April 2020).

Vergne J., Duran R. (2014) Cyberespace et Organisations "Virtuelles": L' état Souverain a-t-Il Encore un Avenir? [Cyberspace and "Virtual" Organizations: Does the Sovereign State Still Have a Future?] *Regards Croisés sur L'Économie*, vol. 1, no 14, pp. 126–39. Available at: https://www.cairn.info/revue-regards-croises-sur-l-economie-2014-1-page-126.htm (accessed 21 April 2020).

Virally M. (1983) La distinction entre textes internationaux de portée juridique et textes internationaux dépourvus de portée juridique (à l'exception des textes émanant des organisations internationales). *Annuaire de l'Institut de Droit International Session de Cambridge*, vol. 60, pp. 166–327.

von Heinegg W. (2012) The Tallinn Manual and International Cyber Security Law. *Yearbook of International Humanitarian Law*. The Hague: TMC Asser Press.

Wall D. (2007) *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity.

Westby J. (2019) Why the EU Is About to Seize the Global Lead on Cybersecurity. *Forbes*, 31 October. Available at: https://www.forbes.com/sites/jodywestby/2019/10/31/why-the-eu-is-about-to-seize-the-global-lead-on-cybersecurity/#6dd3771b2938 (accessed 21 April 2020).

Wheeler D., Larsen G. (2013) *Techniques for Cyberattack Attribution. IDA Paper P-3792, Institute for Defense Analysis.* Available at: https://www.researchgate.net/publication/235170094_Techniques_for_Cyber_Attack_Attribution (accessed 21 April 2020).

Wouters J., Ryngaert C., de Baere G. Ruys T. (2018) *International Law: A European Perspective*. Oxford. Hart Publishing.