Journal of Cyber Policy

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rcyb20

Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?

Dennis Broeders, Els de Busser, Fabio Cristiano & Tatiana Tropina

JOURNAL OF CYBER POLICY
2022, VOL. 7, NO. 1, 97–135
https://doi.org/10.1080/23738871.2022.2041061

Routledge
Taylor & Francis Group

OPEN ACCESS Check for updates

Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?

Dennis Broeders, Els de Busser, Fabio Cristiano and Tatiana Tropina

Institute for Security and Global Affairs, Leiden University, Leiden, The Netherlands

ABSTRACT
This article traces the evolution of interpretations of international law and international cyber norms on responsible state behaviour in cyberspace by reassessing five major – and allegedly state-led – cyber operations: Stuxnet 2010; Belgacom 2013-2014, the Ukrainian power grid 2015, the US presidential election 2016, and NotPetya 2017. Taking recent normative developments and emerging state practices as primary points of refence, it investigates how the current normative landscape can shed light on the nature, (il)legitimacy, and (un)lawfulness of these past operations. For each case, the analysis engages with: i) the elements triggering the violation of norms, principles and international law; ii) the legal and normative significance of recent sources of norms and interpretations of international law; and iii) the legal and political obstacles still lying beyond their application. Taken together, the reassessment of these cyber operations reveals how, in hindsight, the international community has come a long way in calibrating its normative language and practices in calling out irresponsible behaviour in cyberspace. With states taking small, but unprecedented, steps through public attributions and statements on international law in cyberspace, most of the past cyber operations analysed here would arguably feature an attribution in the current climate. At the same time, substantial differences in national interpretations of international law continue to stand in the way of clarity on the terms of its application. In light of this, this article ultimately suggests that cyber norms and the interpretations of international law require further granularity to become 'lines in the sand'.

ARTICLE HISTORY
Received 6 April 2021
Revised 1 October 2021
Accepted 31 December 2021

KEYWORDS
Cyber operations; cyber norms; international law; attribution; diplomacy

1. Introduction

One of the most contested debates in cyberspace is the question of *how* international law applies in cyberspace. Strictly speaking, there exists consensus on the premise *that* international law applies. The UN GGE stated in 2013 that its 'report reflects the Group's conclusion that international law and in particular the United Nations Charter, is applicable

CONTACT Dennis Broeders d.w.j.broeders@fgga.leidenuniv.nl

and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment' (UNGA 2013). This report was consequently adopted by the UN General Assembly. The 2015 UN GGE report (UNGA 2015) reiterated this position and tried to build on it. However, making progress on the matter of how international law applies proved difficult. To a certain extent, the 2015 report worked its way around the difficult question of *how* international law applies by formulating 11 'non-binding rules for responsible state behaviour' some of which echo principles of international law, such as due diligence and human rights protection. The 2016–2017 group of the UN GGE failed to produce a consensus report, with disagreement on how international law applies, and which elements of international law to consider first, as the major bones of contention (see the public statements by Markoff [2017] and Rodríguez [2017]). In 2018, the UN General Assembly was unable to reach consensus on a format for renewed discussions and voted through two resolutions: a Russian-sponsored resolution (UNGA 2018a) calling for the establishment of an Open-Ended Working Group (OEWG) and an American-sponsored resolution calling for the establishment of a new UN GGE (UNGA 2018b). These parallel first committee processes – with almost fully overlapping mandates, but with very different memberships – both resulted in consensus reports in 2021 (UNGA 2021a; UNGA 2021b). Both reports, again, reiterated that international law applies in cyberspace as it does in the offline world, while being unable to take great strides on the issue. The reports did flag new threats as significant and made progress on new norms, and on the details of the existing 2015 norms (see Broeders [2021]). Moreover, the OEWG also produced a Chair's Summary (UNGA 2021d) that contained state proposals that fell short of consensus, while the UN GGE also produced a compendium of state views on the question of 'how international law applies in cyberspace' (UNGA 2021c). Both documents are bound to be on the table when the UN discussion on responsible behaviour in cyberspace continues in the new OEWG (2021-2025) that started its work in December 2021. The French- and Egyptian-sponsored proposal for a Programme of Action (PoA) for cyberspace may also be launched in 2022, potentially providing another UN venue for these discussions (Géry and Delerue 2020).

Outside of international negotiations, states have also been reluctant to specify how international law applies. In most of the instances when states publicly attribute cyber operations, they do not make references to international law, other than in the broadest terms possible (Efrony and Shany 2018; Roguski 2020a). Efrony and Shany concluded that states mostly see the *Tallinn Manual* – a fine-grained analysis by legal scholars on how international law applies in cyberspace – as 'a rule-book on the shelf'. Moreover, they took the failure of the 2017 UN GGE as an expression of '(..) the "wait and see" approach adopted by several states involved in cyber operations in respect of key aspects of the regulatory framework described in the Tallinn Manuals' (Efrony and Shany 2018, 653).[1] In their view, states still had a tendency 'to maintain a policy of silence and ambiguity *vis-à-vis* international law governing cyber operations'. Although some of the recent public attributions of the cyber operations in Georgia to the Russian GRU do take some small steps forward in terms of naming sovereignty and non-intervention as the principles of international law that were violated in the eyes of the attributing state, the overall verdict still is that states are not legally specific when attributing cyber operations (Roguski 2020b).

Legal scholars have been arguing that, for the issue of the applicability of international law to move forward, states need to step up to the plate. Schmitt (2018) states simply that 'ultimately, states need to make a choice' on whether they continue to allow a legal grey zone to exist. Roguski (2020b) concludes that 'when states stop short or leave their views ambiguous, it only encourages further malicious activities by aggressive states'. In the context of attribution and evidentiary standards, Eichensehr (2020) does not mince words when calling for states to do better: 'Evidentiary issues have legal underpinnings, and the U.S., U.K., and French efforts to block the development of customary international law on attribution are short-sighted'. Moreover, the fact that states have not, or have hardly, invoked international law does not mean that there is no 'customary prohibition in this area', in the view of Ohlin (2018, 24). According to him, saying so would merely 'confuse the *identification* of the legal rule with the *application* of that legal rule'. In other words, while the role of states is vital, they are not the only arbiters in the determination of what rule may or may not be applicable.

In the past years, especially between the failed 2017 round of the UN GGE and the 2021 OEWG and UN GGE reports, there has been a lot of activity on matters of cyber norms and on the issue of the applicability of international law. The work on cyber norms 'fragmented' (Ruhl et al. 2020; Broeders and Cristiano 2020) and was taken up in regional multilateral fora (ARF, OSCE, OAS), in private initiatives such as those of Siemens[2] and Microsoft[3] and in multi-stakeholder fora such as the Global Commission on the Stability of Cyberspace.[4] In terms of the applicability of international law in cyber we have three new 'types' of sources: an increasing – albeit still modest – number of states have been releasing statements on how they view the applicability of international law in/to cyberspace. These statements differ substantially from each other, both in legal precision and depth, as well as in the form they take, ranging from official letters to Parliament to speeches (for an overview, see Roguski [2020a]). The recent highlight in this development is the publication of the *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies* as part of the 2021 UN GGE process, which includes 15 state visions on the matter. Another source, albeit it even more modest, is the increasing number of official governments' attribution statements that are starting to contain modest references to international law.[5] Lastly, while the 2019–2021 UN GGE deliberations were traditionally conducted behind closed doors, those of the OEWG were held in public. In addition to the public nature of the OEWG deliberations, the documents that states chose to submit are uploaded onto a public page.[6]

This article takes these various 'new' sources on norms and the applicability of international law as a reference point for a number of 'notorious' cyber operations of the recent past that are suspected to be state-led cyber operations. Would the ongoing debate about norms and the applicability of international law as it currently stands have made a difference in assessing the nature, (il)legitimacy and (un)lawfulness of these operations? In the context of this article, we use 'lawful' and 'unlawful' in relation to (international) law and 'legitimate' and 'illegitimate' in relation to non-binding norms. Would the new thinking on international law and norms have made a difference in terms of the 'language available' for public attribution by the victim state?

In this article we address five cyber operations in this light: Stuxnet (2010), the Belgacom hack (2013-2014), the cyberattacks on the Ukrainian power grid (2015), the interference with the 2016 US presidential election, and NotPetya (2017). These cases were selected for two reasons. Firstly, they are relatively old cases, the latest one from 2017, so they provide sufficient distance from the recent developments in legal and normative thinking. This distance helps with the mental exercise of trying to determine whether these developments provide new language that was unavailable at the time to call out these operations. Secondly, the cases provide a wide spread of cyber operations that were all considered damaging at the political level but are very different in (legal) character. The cases range from sabotage of highly volatile critical infrastructure (Stuxnet), cyberespionage (Belgacom), an attack on critical infrastructure (Ukraine), information operations (the US election) and a very destructive automated cyberattack that borders on vandalism (NotPetya). This variety allows us to take a broad look at the legal and normative developments in the field. Each case will be analysed in three sections. Firstly, what are the component parts of the attacks that may have triggered violations of norms, principles and international law 'regulating' responsible state behaviour? Secondly, do any of the 'new' sources of norms and interpretations of international law provide new lines of 'legal or normative significance' (Ohlin 2018, 5) that could be used to address this case should it unfold today? And thirdly, what lies beyond these possible new lines in terms of legal and political obstacles? Ultimately, the case study analysis along these three lines shows the overall progress in states' thinking about the lawfulness and legitimacy of cyber operations, about legal and normative language used or available for public attribution, and what could be expected in the future.

2. Stuxnet

2.1. Possible triggers for the violation for norms, principles and law

Stuxnet was a multi-model computer worm allegedly developed and deployed by Israel and the United States that sabotaged, between June 2009 and May 2010, the computer systems of five Iranian nuclear facilities located in Natanz.[7] Stuxnet was a highly targeted cyberattack that, using zero-day vulnerabilities, scanned for Siemens STEP 7 software on computers guiding the programmable logic controllers (PLCs) of nuclear centrifuges.[8] Once compromised, those commands caused the centrifuges to spin out of control and destroy themselves. If either Siemens STEP 7 software or a system connection to a PLC was missing, the Stuxnet worm would go dormant inside the computer.[9] As computers in Natanz were air-gapped from the internet, the worm was introduced in the Iranian networks via infected USB flash drives (Kushner 2013).

With no immediate disclosure or attribution coming from either perpetrators or victims, the cybersecurity firm Symantec was first in 'discovering' Stuxnet, once the worm had reached systems outside of Natanz in November 2010 (Falliere, Murchu, and Chien 2010). Evidence gathered in this analysis also indicated the possible involvement of a state because of the worm's level of sophistication, similarity to past cyberattacks, and a clear political motivation (Rid and McBurney 2012). Shortly after Symantec's disclosure, Ali Akbar Salehi – head of Iran's Atomic Energy Organisation – denied that the nuclear plants had experienced any damage, claiming they 'discovered the virus exactly at the same spot it wanted to penetrate because of our vigilance and prevented the virus from harming'.[10] At a later stage, the Iranian President, Mahmoud Ahmadinejad, conceded that some damage had in fact been caused: 'they succeeded in creating problems for a limited number of our centrifuges with the software they installed in electronic parts' (Brown 2011).

While neither Israel nor the United States has ever officially claimed, nor denied, responsibility for the attack, in 2012 a *New York Times* investigative report confirmed these allegations and exposed Stuxnet as a joint US-Israeli operation.[11] Iranian authorities made their official public attribution only in 2013 when the commander of the national civil defense, Gholam Reza Jalali, declared to the Iranian state news agency (IRNA) that 'after following up the reports that were sent, it became clear that the attackers were the Zionist regime and the American state of Texas' (*Jerusalem Post 2011*). Besides the Iranian late attribution, the international community remained silent with regards to the public attribution of Stuxnet. The unsettled question regarding state attribution has hindered the possibility of any application of international law – in as much as any action by Iran or the international community would have been unlawful without clear attribution to a sovereign entity (Efrony and Shany 2018).

2.2. New lines of legal or normative significance?

In 2010, Stuxnet, for the first time, brought general attention to the question of *whether* international law could be applied to cyberspace (Farwell and Rohozinski 2011; Richmond 2012; Richardson 2011). At this point, the academic debate focused primarily on assessing whether Stuxnet violated Article 2(4) of the UN Charter on the prohibition of threat or use of force; whether it constituted an armed attack under the meaning of Article 51 of the UN Charter; or whether it initiated an international armed conflict under international humanitarian law. According to customary interpretations of Article 2(4), armed force requires kinetic weaponry, wherein the term 'weapon' refers to a tool that causes effects of a physical nature on a body or on an object.[12] Back in 2010, there existed disagreement on whether the UN Charter alone could also provide sufficient grounds for classifying Stuxnet as armed force; the worm sabotaged the SCADA systems through the manipulation of data, and whether it had caused effects of a direct and univocal physical nature remains debated (Fidler 2011; Peagler 2014).[13] Stuxnet thus tested the ability and limitations of standing international law to regulate cyber operations and served as an important empirical reference for the drafting of the 2013 Tallinn Manual (Peagler 2014). A first contribution made by the manual was in fact to clarify that 'as illustrated by the Stuxnet incident, significant legal and practical challenges stand in the way of definitively concluding that a cyber operation has initiated an international armed conflict' (Schmitt 2013, 84). While the International Group of Experts agreed that Stuxnet amounted to use of force, there was no agreement on whether it met the armed attack threshold (Schmitt 2013, 58). The authors of the Tallinn Manual also added that Stuxnet violated the principle of non-intervention 'because all uses of forces are coercive per se' (Schmitt 2013, 45).[14]

Building on new empirical evidence, and on the analysis put forward in its first edition, the Tallinn Manual 2.0 in 2017 further advanced the debate on the application of international law and again made reference to Stuxnet, both explicitly and implicitly. With regards to the prohibition of use of force, the second version of the manual clarified that 'neither physical damage nor injury is required for a cyber act to be an internationally wrongful act' and, through Rule 69, that the threshold of use of force is reached when a cyber operation's 'scale and effects are comparable to non-cyber operations rising to the level of a use of force' (Schmitt 2017a, 45). While agreeing on the fact that Stuxnet constituted an unlawful use of force, the experts continued to disagree on whether Stuxnet amounted to an armed attack (Schmitt 2017a, 342) and whether a cyber operation such as Stuxnet could initiate an armed conflict (Schmitt 2017a, 384; on this, also see Kilovaty [2014]).

As Stuxnet damaged a national critical infrastructure, today it would also be considered in violation of UN GGE 2015s norm 13 (f) that condemns attacks on critical infrastructures. Similarly, this issue has been put forth by the Paris Call that condemns cyberattacks 'threatening or resulting in significant, indiscriminate or systemic harm to individuals and critical infrastructure', this way 'softening' the physical damage requirement that had characterised initial debates around Stuxnet. As Stuxnet substantially sabotaged elements of the country's critical infrastructure systems and attempted to coerce Iran into diverting or abandoning its nuclear plans, it provides further grounds for considering this operation a violation of the principle of non-intervention (Denning 2012). Interestingly, the Tallinn Manual 2.0 specifies that 'the fact that uncertainty remains as to the originator of the operation does not preclude its qualification as intervention, should it later be reliably established that it was conducted by a State' (Schmitt 2017a, 327). Regardless, the question of attribution of the Stuxnet worm continues to be addressed across international cyber norms processes and diplomacy. In the 2019s submission to the OEWG, Iranian representatives stated that the country 'is among the first targets when attacked in Stuxnet case' and thus warned against the risk that 'certain States with offensive doctrines violate the prohibition of the use of force against other countries as enshrined in the UN Charter' (Islamic Republic of Iran 2019).[15]

In 2013, the UN GGE put forth a recommendation on international law stating that 'state sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory' (UNGA 2013, 8). Along the same lines, Tallinn Manual 2.0's rule 4 on sovereignty stated that 'in the cyber context, therefore, it is a violation of territorial sovereignty for an organ of a State, or others whose conduct may be attributed to the State, to conduct cyber operations while physically present on another State's territory against that State or entities or persons located there' (Schmitt 2017a, 19). As an example, the Manual 2.0 referred to a circumstance comparable to Stuxnet: 'For example, if an agent of one State uses a USB flash drive to introduce malware into cyber infrastructure located in another State, a violation of sovereignty has taken place' (Schmitt 2017a, 19). While the earlier academic debate on the application of international law to the case of Stuxnet had overlooked the issue of sovereignty, Tallinn 2.0 made an important contribution by bringing it to the table. At the same time, the USB-drive argument appears, to say the least, very limited when compared to recent developments wherein states invoke the sovereignty principle for cyberattacks of lower intensities, such as the accusation made by Germany in relation to the 2015 cyberattack on its parliament, or in the sovereignty debate surrounding the 2019 Russian cyberattacks on Georgia's governmental agencies (conform Roguski 2020b).

2.3. Legal obstacles and possible ways forward

More than 10 years after Stuxnet, a lot has changed in the discourses surrounding responsible state behaviour in cyberspace (Segal 2016). Stuxnet served as a fundamental point of reference for the overall debate and was an empirical inspiration for the first Tallinn Manual. The second version of the manual (2017) provided enough grounds to categorise Stuxnet as a violation of the prohibition of the threat or use of force, a threshold that remains, however, generally high for cyber operations. When considering this restrictive understanding of the use of force, Stuxnet is in fact considered the only cyberattack to have clearly met the requirements for being considered an unlawful use of force (conform Delerue 2020). Stuxnet's never-repeated magnitude has ever since shaped the normative process with interpretations of international law placing a high bar for the different thresholds.

Looking back at Stuxnet in light of recent developments on the issue of sovereignty (discussed later in this article), it can be argued that little today would stand in the way of its recognition as a violation of Iranian territorial sovereignty. As already argued by Roscini in 2014, 'cyber-attacks like Stuxnet are, as a minimum, a violation of the sovereignty of the target State' (Roscini 2014, 72). Whereas Tallinn 2.0 in 2017 offered clear grounds to assess Stuxnet as a violation of Iranian sovereignty – primarily because of the USB-pen controversy – today's debate has moved as far as countries like France considering 'any unauthorised penetration' of their systems to be a violation of sovereignty, regardless of its actual damages, or let alone the presence of a foreign agent on the target country's territory (on this debate, see Schmitt [2020]; Buchan [2020]). This means that, with defacement attacks on Georgia being met with a large public attribution coalition of over 15 countries (some of which are invoking violations of sovereignty), it appears hard to believe that Stuxnet would not trigger, at the very least, a similar response (conform Nakashidze 2020; Roguski 2020b).

3. Belgacom hack

3.1. Possible triggers for the violation for norms, principles and law

Assumed to have been active since approximately 2011, the reportedly highly sophisticated intrusion of Belgacom's systems was discovered by the company between 2012 and 2013 (Marquis-Boire, Guarnieri, and Gallagher 2014). Belgacom is Belgium's largest telecommunication company servicing the Brussels-based EU institutions and NATO headquarters. It also has a subsidiary company by the name of Belgacom International Carrier Services (BICS) that has partnerships with many telecommunications companies in the rest of Europe, US, Asia, Africa and the Middle East. This makes the corporation an interesting target for wide-ranging surveillance purposes, including access to political or military targets. That fact in itself, plus the sophisticated level of the intrusion, raised early suspicions of a state actor (Gallagher 2014, 2018). No customer data was stolen, nor were services interrupted (Belgacom 2013).

The Belgian government at first reacted strongly, calling the act a 'breach of the integrity of the public[16] company' (De Standaard 2013). Belgacom filed a complaint with the federal prosecution authority. Yet when information became available on the possible involvement of the GCHQ and the NSA, criminal prosecution became more and more unlikely. *Der Spiegel* published documents revealed by NSA whistle-blower Edward Snowden, including a presentation by GCHQ's Network Analysis Centre labelled as 'top secret'. The slides mention Belgacom and BICS as the targets of 'Operation Socialist' with the ultimate goal of enabling computer network exploitation access to Belgacom Core GRX routers ‘from which we can undertake man-in-the-middle operations against targets roaming using smart phones’ (*Der Spiegel International* 2013). This revelation was not followed by an official attribution by any member of the Belgian government or law enforcement apparatus, nor by the company itself. Five years later, the criminal case was dismissed due to insufficient evidence, according to a confidential federal prosecution report to which journalists had access (De Morgen 2018).

Two possible triggers for the violation of norms, principles and law can be distinguished in the Belgacom hack: one, it constitutes an act of *cyberespionage* and two, it constitutes an act of espionage between (then) EU and NATO *allies* (Boeke and Broeders 2018, 76).

First, media referred to the hack as a case of digital espionage by the UK’s GCHQ (*Der* Spiegel 2013; Gallagher 2014). The Belgian government never publicly called it an act of espionage but confirmed the possibility of the involvement of another state and the purpose of collecting strategic information (De Standaard 2013). No reference was made to a breach of sovereignty or any other rule, principle or norm. The UK involvement could explain why the Belgian government – the country being a relatively small player on the international stage and requiring the assistance of the UK and the US in other international cases, especially the fight against terrorism – refrained from publicly attributing the hack to the GCHQ.

Second, the UK is considered a long-time ally with whom Belgian authorities cooperated in the EU and NATO frameworks. Moreover, the UN GGE makes it a norm for states to cooperate with each other in exchanging information and assistance and prosecuting criminal use of ICTs.[17] In general, cooperation in criminal matters *between EU member states* is rooted in tradition and trust. Although at first the UK was one of the driving forces of the stronger cooperation within the area of freedom, security and justice, it has gradually shown a more reluctant attitude towards collaboration (Brière 2020).[18] When Belgian investigative authorities requested assistance from the British Home Office in identifying the users of relevant IP addresses, the response was that this could endanger the British sovereignty, security and public order (De Morgen 2018). The latter is a ground for refusal traditionally used in mutual assistance in criminal matters[19] but vague and wide-ranging enough to act as a safety net that countries can rely on when they do not wish to deliver the requested assistance. In aftermath of the Belgacom hack, such a response is meaningful because relying on sovereignty, security and public order as a way of refusing to reveal the identity of specific IP address users indicates that these users are not the average citizens, rather individuals in need of some form of special protection. Journalists said that prosecutors called this an exceptional situation between EU member states and one which could potentially lead to a diplomatic incident (Vanhecke and Eeckhaut 2018).

Europol equally refused assistance upon a request by Belgian police authorities, citing its limited mandate (Gallagher 2018; see also Regulation [EU] 2016/794). Sources revealed that Europol refused to get involved in investigations alleging an attack by the UK (Gallagher 2018). As Europol’s mandate has always been restricted to criminal investigations, acts committed by governments are excluded by definition (Regulation [EU] 2016/794). Moreover, where most EU member states maintain a clear separation between police and intelligence authorities and the information they gather (Vervaele 2005, 3–5), EU institutions and agencies have no power whatsoever in national security issues, which remain solely a matter for national governments. *A contrario* one could take this as an indication that the case not falling within the mandate of Europol is a non-criminal, and thus national security, investigation.

3.2. New lines of legal or normative significance

No clarity exists on whether an act of cyberespionage is allowed or not.[20] International law on peacetime espionage is not fully formed (Schmitt 2017a, 25) and the current norms on responsible behaviour in cyberspace do not mention espionage. However, what is new in this discussion is the shift in response. States and international organisations are moving from remaining silent on the activities by states' intelligence agencies to addressing them, at times even publicly. Recently, such an attribution was made by Chancellor Merkel, highlighting hard evidence for Russia's responsibility in hacking the German parliament, followed by an international arrest warrant for a GRU employee (Von Der Burchard 2020; see also BBC News 2018). In 2013, the European Commission and Parliament called the spying on EU offices by the US unacceptable (BBC News 2013a). The German intelligence service was caught spying on allies, on UN offices and on NGOs (Minns and Brown 2015) two years after Merkel's fierce reaction to US access to her phone (BBC News 2013b). With regards to international organisations such as the UN, espionage in peacetime goes back as far as the negotiating of the UN Charter in 1945 (Schlesinger 1995; see also Davis and Isenberg [2003]).

The lawfulness of (cyber)espionage is murky territory, regardless of whether an international organisation or a state is the target, yet the scholarly discussion that follows sheds some light on the matter (Navarrete and Buchan 2019, 903; Wrange 2014, 321). Delerue (2020, 200) summarises it as follows: 'the lawfulness of cyber espionage activities is no different from the lawfulness of other cyber operations: there is no general prohibition of cyber espionage, but the cyber operations used may breach specific norms of international law'. Of those specific norms, the violation of sovereignty seems the most relevant approach, considering the absence of force. Yet, identifying criteria for such violation is much harder. Some scholars consider *any* unauthorised exercise of authority in another state a breach of sovereignty (Buchan 2018, 49–55). This wide view, however, would render most intelligence-gathering activities unlawful (Moynihan 2019, 20; see also Egan [2017, 174]). Other scholars – such as the Tallinn Manual 2.0 experts – support the idea that a threshold of damage should be applied, but do not agree on the severity of the damage (Moynihan 2019, 27; Schmitt and Vihul 2017a, 218). The three degrees of damages they distinguished ranged from physical damage (as in Stuxnet) or injury to the loss of functionality of cyber infrastructure and activity below the loss of functionality (Moynihan 2019, 21; Schmitt 2017a, 20–21; Lubin [2018, 215–219]; Navarrete and Buchan 2019, 907). Other authors do not use the damage threshold (Wrange 2014, 321) nor have they indicated further criteria. Corn and Taylor refer to a state's right to conduct necessary national security operations by means of espionage such as the gathering of information on terrorist organisations (Corn and Taylor 2017, 211).[21] Lubin describes the *just causes* of spying: national security and international stability and cooperation (2020, 231–242). The reasoning developed by Lubin also contains four *unjust causes* or categories of unlawful espionage: spying as a means to advance personal interests; spying as a means to commit internationally wrongful acts; spying as a means to advance corporate interests; and finally, spying as a means to exploit post-colonial relations (236-242). When studying the Belgacom hack, the question arises as to whether it would fall under the just or the unjust causes of spying.

Unpacking that question, we look again at Lubin, who labels spying when used as a tool to commit internationally wrongful acts as unlawful, based on its purpose and its context. This means that if espionage is the constitutive element in a larger wrongdoing to the point where one can no longer separate the intelligence gathering from the wrongful act, the intelligence gathering is also unlawful (Lubin 2020, 239). The conclusion resembles the argument by Jupillat (2017, 979–984) stating that the scale and context of such operations matters. This perspective could accommodate both the above-mentioned damage threshold and the preservation of necessary operations. If the context of cyberespionage is a terrorist investigation or a benign intelligence gathering, the operation is lawful and does not breach the target state's sovereignty (Corn and Taylor 2017). If the context reveals a malicious act such as election interference (Jupillat 2017, 982–983) or annexation (Lubin 2020, 238), the operation is unlawful. Following this reasoning – and based on the limited public information – the Belgacom hack would be a benign gathering of intelligence. Obviously, knowledge of the larger context requires information – that the victim state does not necessarily have – but the purpose-approach seems promising in moving forward the debate on the lawfulness of cyberespionage. Provided ample information is available, such an approach gives clearer results than the above-mentioned damage threshold.

A few governments have taken a stance by making statements on sovereignty, sometimes at the occasion of a public attribution (Roguski 2020a, 4–7). None of them directly address espionage. Rather, they hover over the topic of sovereignty, leaving room for interpretation – except the French statement. The French government called any unauthorised penetration of 'French systems' a breach of sovereignty but explicitly left cyberespionage out of the scope of their statement. Regarding cyberespionage, the statement clarifies in a footnote that it is not unlawful in international law but may breach it when linked with an international wrongful act (Roguski 2020a, 5; French Ministry of the Armies 2019, 4). Thus, this view would label the above-mentioned benign intelligence-gathering operations as lawful. The UK Attorney General, Jeremy Wright, asserted in May 2018 that he is 'not persuaded that we can currently extrapolate from that general principle [of sovereignty] a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention' (Wright 2018). Roguski (2020a, 4–5) calls this the sovereignty-as-a-principle approach that leads to certain cyber operations falling outside of the scope of international law breaches. The UK's view on sovereignty would in fact align with the idea that the actions by the GCHQ are allowed. Other states that came forward with a view on sovereignty and cyberspace are not specifying any further criteria (Roguski 2020c; Hollis 2020a, 2020b). The Netherlands stuck to the Tallinn Manual and Germany and the US are unclear in their positions (Roguski 2020a, 5–6; see also Ney 2020). Belgium has so far not made any statements in that context.

Besides the difficulties with defining cyberespionage, the Belgacom hack also exposed an incident between two allies followed by a refusal to assist in investigating the case. The norm of cooperation between states that need each other's assistance is essentially a wide-ranging norm that can encompass cooperation in all shapes and sizes. When the UN GGE norm d provides that 'states should consider *how* best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats', it does not specify that the channel of criminal prosecution must be used. The same goes for the norm proposed by the Digital Geneva Convention. Theoretically, one could state that diplomatic efforts, such as the meetings in the months after the hack, comply with this norm. Recognising that the roots of mutual legal assistance in criminal matters lie in diplomatic traffic, this would not be too far-fetched (De Busser 2017, 81; Nilsson 2006, 53–54).

3.3. Obstacles and the way forward

Scholars, as well as a minority of governments, are making attempts at determining whether an act of cyberespionage is lawful via the approach of a sovereignty breach. On a government level, sovereignty has surfaced in public attributions but there is still a significant lack of criteria for determining when exactly a breach occurs. Apart from a few exceptions (Von Der Burchard 2020; BBC News 2018), states seem hesitant to make progress on this issue. A noticeable and more recent exception is the public attribution, in April 2021, by the Biden administration, of the SolarWinds Orion incident. Formally naming the 'Russian Foreign Intelligence Service (SVR) – also known as APT 29, Cozy Bear and The Dukes' as the responsible party, the US released a list of responses to what they refer to as actions against US sovereignty and interests (White House 2021). Scholars refer to the incident as a relatively proportionate espionage operation and call out the list of responses as a clever way to react more robustly against a variety of Russian activities (Devanny, Martin, and Stevens 2021). The White House's statement, however, unambiguously refers to the incident as a 'broad-scope cyber espionage campaign'. The novelty not only lies in the clarity of the language used but also in the introduction of a multi-factor test for responding to cyber incidents (Eichensehr 2021). Such factors include the scope of the incident, the burden on the private sector, the history of the perpetrator causing disruptive cyber operations, the risk to the global supply chain and the theft of 'red team' tools (White House 2021). No clarity is offered on whether these factors should occur cumulatively or contain some form of hierarchy (Eichensehr 2021), but the reasoning seems to be one of a risk-based approach. The Biden administration highlights the likelihood of harm flowing from the SolarWinds Orion incident. This means that such an espionage campaign does not have to result in clear and present damage to trigger a response, the risk of damage is sufficient. Alongside the statement by the US, the UK's NCSC made a public attribution of the incident to Russia as well, although their statement does not refer to espionage but to a 'pattern of malign behaviour' (United Kingdom's Foreign, Commonwealth & Development Office 2021).

On an academic level, progress seems to be made by moving away from the damage threshold and finding (un)lawfulness in the purpose of the espionage. The damage threshold supported by the Tallinn Manual would not qualify the Belgacom hack as an unlawful breach of sovereignty since the hack did not lead to any direct impact on customers. Still, the company spent €50 million in cybersecurity measures in the aftermath of the hack (Belgacom 2013; De Morgen 2018; European Parliament 2013). Determining the lawfulness of the hack by assessing its purpose, there are no clear indications what the collected strategic information would be used for. However, the media exposed that several meetings between Belgian and British diplomatic staff happened in the months after the hack, including even a two-day conference of both Ministers of Foreign Affairs in London and a meeting between the British Ambassador and the Belgian Federal Prosecutor (Modderkolk 2018). This seems to show a breach of trust between two (then) EU member states and, in combination with the dismissal of the criminal prosecution, may indicate that both parties mended that trust and concluded that the hack was a lawful intelligence operation. In order to avoid such diplomatic incidents between two states, it would be helpful to gain more clarity on the necessity requirement. The general idea behind this requirement in the context of surveillance is that operations are necessary when the same result cannot be achieved with less intrusive means (EDPS 2017, 7–9). Possibly such a standard could be used for the purpose of distinguishing a lawful from an unlawful cyberespionage operation as well; if the same information could, for example, be gathered by using classic human intelligence, then the operation is unnecessary and, therefore, unlawful.

Clarifying the question of the lawfulness of cyberespionage will increase states' trust in each other's actions. An additional confidence-building measure is the development of national law and oversight mechanisms on intelligence services. Currently, pressure on states is mounting to increase transparency regarding, and oversight of, their own intelligence agencies, largely because of the scale and pervasiveness of cyberespionage (Broeders, Boeke, and Georgieva 2019; Moynihan 2019, 44–45; Navarrete and Buchan 2019, 922). That, together with initiatives increasing cooperation between national oversight committees, could pave the way forward in this debate.

4. The Ukrainian power grid

The attack on the Ukrainian power grid in 2015 was the first publicly documented cyberattack against critical infrastructure that led to a power outage (FireEye 2016) and the first known attack on an energy grid carried out completely remote ("Power grid cyberattack" 2019; McLellan 2016). It started on 23 December 2015, with the illegal entry of a third party into the SCADA systems and computers of the electricity distribution company Kyivoblenergo. Malicious actors obtained credentials and gained access to the energy substation networks via spear-phishing emails to install BlackEnergy3 malware,[22] which allowed them to cut power remotely. Furthermore, the attackers erased data on infected computers with the payload KillDisk (Baezner 2018, 15) and started a 'Denial-of-Service' attack over the telephone to block the lines for real customers as a part of covering any aspect of the highly sophisticated scenario (Zetter 2016a). 30 distribution substations were disconnected for three hours, and operators were forced to switch into manual mode (E-ISAC 2016). The disruption affected several distribution companies, resulting in power outages for 225,000 customers (Rõigas 2018).

The severity of the attack and the fact that it impaired the operation of a civilian critical infrastructure – the power grid – could potentially constitute triggers for violation of international law, principles and norms. The response to the attack, however, never got anywhere near the debate on the applicability of international norms, let alone their enforcement, due to uncertainty in attribution and the absence of coordinated actions.

According to some media sources, the Ukrainian government almost immediately pointed at Russia as a possible source of the attack (Kovacs 2015; Nakashima 2016; Hern 2016), yet the official attribution was postponed pending the results of investigation

(Polityuk 2015). In January 2016, the US Department of Homeland Security stepped in to help with investigating the case (Volz and Finkle 2016),[23] but this involvement never resulted in an official attribution. The only attribution was provided by the US private cyber intelligence company iSIGHT Partners[24] which linked the operation to Russia, claiming that it was executed by a group known as 'Sandworm' (Newsweek 2016; FireEye [2016;] Hultquist 2016) with the use of BlackEnergy malware. However, there has been no unified position among cybersecurity experts on the link between BlackEnergy and Russia. The US Department of Homeland Security issued an ICS-CERT alert acknowledging the use of this malware in the attack, however, without official attribution to Russia and with a reservation that 'the role of BlackEnergy in this incident is still being evaluated' (CISA 2016).

The Sandworm group is widely believed to be connected to the Russian government, and in recent years some of the official statements clearly refer to this link (see, e.g. the alert issued by the US CERT [CISA 2020]). It is not entirely clear why Ukraine and other states haven't tried to pursue an official attribution nor a response that would have referenced international law. Some researchers argue that attribution itself was a problem because of the lack of distinction between state and non-state actors, who seemed to share the tools for attacks (Baezner 2018, 12). Furthermore, some opine that even though the attackers could have caused much more damage (Zetter 2016b), they deliberately avoided crossing what Lin (2012) refers to as 'lines in the sand', in keeping an attack below the level that would provoke a 'significant response from Ukraine and its allies' (Baezner 2018, 16).

4.1. New lines of legal or normative significance

The issue of how international law can deal with cyberattacks against critical infrastructure has been widely debated in recent years. However, the applicability of the particular norms to the Ukrainian power grid incident would depend on whether this cyber operation happened during an international armed conflict or peacetime. The incident happened after the annexation of Crimea by Russia and during the time of military actions in the Ukrainian regions of eastern Donetsk and Lugansk (see, e.g. Park, Summers, and Walstrom [2017]). While Russia denies the international nature of the conflict and its military presence in Ukraine and considers it to be Ukraine's internal conflict (Merezhko 2018, 112), academic scholars (Schmitt 2017b; Valuch and Hamulak 2018; Merezhko 2018, 112) and international organisations (OSCE 2015; ICC 2016, 37) consider the military actions in the Ukrainian regions of eastern Donetsk and Lugansk as an armed conflict between Russia and Ukraine.

4.1.1. Attacks against critical infrastructure during armed conflict

If considered an international armed conflict, the question becomes whether a cyberattack against the Ukrainian power grid falls under the Article 49 of the Additional Protocol I to the 1949 Geneva Conventions, which construes an attack as 'act of violence against the adversary, whether in offence or in defence'. There exists no unanimous position on the application of Article 49 of the Additional Protocol I to those attacks that do not cause physical damage and result in impairment, such as loss of functionality (ICRC 2019, 7), however, the recent interpretations increasingly argue in that direction. Cyber operations causing physical damage, death or injuries constitute an attack under IHL. Moreover, according to some recent interpretations of Article 49, it appears likely that most cyber operations which, regardless their scale and intensity, generally do not cause physical damage, would also qualify as attacks under IHL. The ICRC, for example, considers 'an operation designed to disable a computer or a computer network' to be an attack under Article 49, because otherwise the restrictive notion of the attack contradicts the essential principle of protecting civilians (ICRC 2019, 7–8). Schmitt admits that a strict interpretation of the definition of attack under IHL would only put 'cyber operation causing damage to objects or injury to individuals' under the scope of the Article 49, and this would seemingly exclude the attacks against the Ukrainian power grid from limitations and prohibitions established by IHL. However, he argues that such exclusion would counter the purpose of IHL due to under-inclusiveness of cyberattacks that could have the same effect as kinetic attacks in putting the infrastructure out of operation, but without physically damaging them (Schmitt 2017b, 17).

States, in their interpretation of the principles of IHL, started following the same line of argument. For example, France's official position on the application of IHL to cyber operations is that an operation in cyberspace during wartime would constitute an attack under Article 49 when 'the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not', even in the cases when 'there is no human injury or loss of life, or physical damage to goods' (French Ministry of the Armies 2019, 13). These broader interpretations of Article 49 would allow for extension of the principles of the IHL that protect the civilian population from the cyber operations amounting to an attack. Such an interpretation has notably been brought forward in the 2019, in the French position on the international law applied in cyberspace (French Ministry of the Armies 2019, 14). Consequently, the cyber operation against the Ukrainian power grid is likely to fall within the definition of an attack as provided by Article 49. In that case, this (cyber)attack, which targeted a civilian infrastructure, may have breached the principle of distinction which makes it necessary to distinguish civilians and civilian objects from military objective, notably defined by Article 52 of the Additional Protocol I, the latter being the only lawful targets of attacks. This article establishes a two-pronged test to determine whether an object is to be considered a military objective (Pilloud et al. 1987, 635). As the first prong, the object must 'make an effective contribution to military action' of the enemy. As the second prong, the object's 'total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage' for the attacking side. The Ukrainian power grid is unlikely to constitute a military objective following the two-pronged test. Therefore, if the cyber operation against the Ukrainian power grid is considered as an attack according to Article 49, it is likely to be considered unlawful since it was not targeting a military objective. Furthermore, this operation could constitute a violation of the principle of necessity, which establishes that weakening of military capacity of the other party is the only legitimate purpose in the case of an armed conflict (Sassoli et al. 2014).

4.1.2. Attacks against critical infrastructure during peacetime

Concerning the applicability of peacetime's international law to the cases of the attacks against critical infrastructure, the literature points to the possibility that attacks against critical infrastructure could violate principles of sovereignty and non-intervention (Moynihan 2019). Government approaches to violation of sovereignty, however, differ significantly. While some states, like France, consider any attack against French digital systems to be a breach of sovereignty, others, like the United Kingdom, argue that the general principle of sovereignty cannot lead to a 'specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention' (Roguski 2020a, 4).

Attacks against critical infrastructure in peacetime also fall under the norms suggested in the 2015 UN GGE report. The nature of the target in cases similar to the Ukrainian power grid attack – utilities – warrants potential applicability of the non-binding norm 13(f), which affirms that states should not conduct or knowingly support ICT activity that aims at damaging critical infrastructure. Other sets of non-binding norms adopted after the 2015 attacks on the Ukrainian power grid, such as the Paris Call for Trust and Security in Cyberspace (Paris Call 2018) and the Global Commission on the Stability of Cyberspace report[25], could also be considered in case of similar cyber operations. While the Paris call condemns malicious cyber activities against critical infrastructure, its norms focus rather on the prevention of, and recovery from, such incidents. The GCSC proposed that non-state actors should not engage in offensive cyber operations. Yet, all these norms are not legally binding; there would be a need for political will to reference them in response to the attack. Furthermore, as a part of recent developments, both the 2021 GGE and 2021 OEWG reports stress the importance of protection of critical infrastructure in peacetime. This underlines the willingness of the states to ensure that non-binding norms provide agreement on its protection against cyberattacks in peacetime.

The applicability of the peacetime cyber norms to the case of Russian attacks against Ukrainian critical infrastructure, however, can be debated only in theory, as the existence of an armed conflict would prevent their application. For example, Michele Markoff, Coordinator for Cyber Issues, US Department of State, reportedly asserted that the attack on the Ukrainian power grid could not be considered a violation of the GGE norms, because the US government considers Russia and Ukraine to be in a state of open conflict (see Marks [2017]; see also Markoff et al. [2017]).

4.2. Legal obstacles and possible ways forward

The case of the Ukrainian power grid raises several issues with regard to the possible way forward in addressing attacks against critical infrastructures. The possible triggers and consequences for the application of international law and norms would be different depending on whether the attack happens during peacetime or armed conflict. For the latter scenario, the broader interpretation of the attack under the Article 49 of the Additional Protocol I, already suggested by scholars and the ICRC, would consider cyber-attacks against civilian infrastructure during wartime to be a violation of the IHL principle of distinction and, therefore, of other principles such as necessity, proportionality and precaution.

With regard to the cyber operations against critical infrastructure in peacetime, there exists growing awareness among states about the necessity to pursue international law or norms in response to these attacks. One of the possible routes is triggering the rules on respect for sovereignty. However, in case of non-destructive attacks against critical infrastructure, as pointed out by scholars, such application is controversial (Cyber toolkit, scenario 3 2020) because of the difficulties in 'drawing the line for a *de minimis* threshold based on the effects in the target state' (Moynihan 2019, 22). This has not stopped countries such as France putting forward opinions that any attack can constitute a violation of sovereignty (Roguski 2020a, 4), but it is not very likely that many other states will follow this approach.

In the absence of a unified position among states concerning the applicability of an obligation to respect sovereignty – to cyberspace in general and to critical infrastructure – the second possible route is the reference to the non-binding norms in states' responses to the attacks. This could include the norm 13(f) of the GGE 2015 report, the Paris Call's references to attacks on critical infrastructure or, and perhaps even the GCSC norm on non-engagement in offensive cyber operations. For example, US State Secretary Pompeo recently referred to the non-binding norms of GGE 'regarding states refraining from cyber activities that intentionally damage critical infrastructure' in condemning attacks on hospitals in the Czech Republic (Pompeo 2020). However, there are scholars, like the authors of the Cyberlaw Toolkit, who argue that 'the legal valence of any normative statements' in the UN GGE reports 'must be understood as minimal to none' (Cyber toolkit, scenario 3 2020). The use of non-binding norms in response to the attacks would, therefore, constitute a political message that draws attention to the states not adhering to voluntary norms in the absence of legal tools to enforce them. However, according to some views, such political messages, if they are sent in a coordinated and consistent manner, can be one of the steps in changing 'the new normal of 'anything goes'' (Hathaway 2017, 6).

5. Interference in the 2016 US presidential elections

5.1. Possible triggers for the violation for norms, principles and law

The events and timeline of the suspected Russian inference in the 2016 US presidential election have been extensively documented in official US government reports (ODNI 2017; Mueller 2019) as well as in scholarly articles (see, e.g. Efrony and Shany [2018, 609–617]; Kilovaty [2018, 152–157]; Schmitt [2018, 33–39]; Egloff [2020]; Hall Jamieson [2020]). For the purposes of this article, we focus on those elements of this campaign that can conceivably trigger a violation of norms, principles and laws.

Three interrelated events/operations make up the Russian interference with the US presidential elections in 2016. The first is the hack of the Democratic National Congress and the subsequent release of emails and documents ('the DNC hack'). The second is the hack of the email account of John Podesta, then chairman of Hilary Clinton's presidential campaign, and the leaking of those emails. The third is the online 'trolling campaign' on social media aimed at influencing the thinking of American voters. In terms of possible lines of legal or normative significance, the first two are similar, whereas the online trolling campaign raises very different questions.

The main offences in the first two operations are gaining unlawful entrance to DNC systems and Podesta's email account through spear-phishing and/or hacks and the subsequent release of the stolen data through the Guccifer 2.0 persona, DCLeaks, WikiLeaks and some exclusive releases to the media (Schmitt 2018, 34). The releases were timed to create optimal political effects: just before the Democratic Party Convention; just after the release of the audio tape of Donald Trump on *Access Hollywood*, in which he made degrading comments about women; and just before the presidential election itself. The intent was clearly to disrupt legitimate domestic democratic processes (Kilovaty 2018, 155–156).[26] The legal triggers in the hacks and leaks are gaining unauthorised access, stealing, and releasing data in bulk, all of which are illegal under domestic law. The trolling campaign, using social media platforms to sow division and heighten nativist tendencies, is flagged by some scholars because of the fact that Russian actors impersonated American citizens and organisations (Ohlin 2018, 5; Schmitt 2018, 51). The covertness of these impersonations of citizens makes the trolling legally significant to those authors.

The official US government's attribution of the attacks to Russia took place in January 2017. The joint report of the CIA, FBI and NSA, under the auspices of Office of the Director of National Intelligence (ODNI), named the Russian government (the GRU) and non-government operatives (such as the IRA) and stated that 'Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election' (ODNI 2017, ii; Schmitt 2018, 33). The CIA and the FBI made the attribution with a 'high degree of confidence'. The NSA concurred, but only with a 'moderate' degree of confidence (Schmitt 2018, 34).

Although states have expressed dismay about election interference, in legal terms they have failed to do justice to what is an attack on 'the most sacred of domestic affairs' (Nicolas 2018). If democratic elections are at the heart of what it means to be a liberal democracy, then the official US government reactions look pale in comparison to the crime (Broeders 2020). In terms of calling out 'legal lines of significance', the US government has mainly done so through domestic criminal law, but not through international law. In December 2016, the White House issued a presidential statement indicating that '[t]he United States and friends and allies around the world must work together to oppose Russia's efforts to undermine established international norms of behaviour and interfere with democratic governance' (Efrony and Shany 2018, 615). Efrony and Shany rightly ask, but do not answer, the question of whether this means that the US is signalling that influence campaigns are in violation of international law governing cyber operations, or that the US took the position that they violated 'informal norms governing state conduct in cyberspace' (615). The US silence on international law is echoed by the fact that all the measures taken in response to the election interference[27] – sanctions and declaring people *personae non grata* – do not rise above the level of retorsion, unfriendly measures that do not require any prior violation of international law to be considered lawful.

5.2. New lines of legal or normative significance?

International lawyers have been grappling with the fact that states have not yet called out election interference through cyber means as a violation of international law. Legal scholars have been looking into sovereignty and the principle of non-intervention as possible avenues for identifying 'lines of legal significance'. Additionally, in recent years there has been some new thinking on these matters in terms of norms and legal interpretations that help with identifying lines of legal and normative significance.

Even though states have not mentioned international law in any public attribution yet, they increasingly flag election interference as a possible breach of international law, or more specifically as a breach of the non-intervention rule (see Roguski [2020a] for an analysis). In the run-up to the UN GGE and OEWG 2021, an increasing number of countries have set out their views on how international law applies to state conduct in cyberspace. Some of these explicitly mention election interference as a possible breach of non-intervention. The Netherlands, echoing the Nicaragua case, defines intervention as 'interference in the internal or external affairs of another state with a view to employing coercion against that state' and explicitly states that 'National elections are an example of internal affairs' (Kingdom of the Netherlands 2020a). The UK holds that 'the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state' would 'surely be a breach of the prohibition on intervention in the domestic affairs of states' (Wright 2018). Brian Egan, legal advisor to the US government, stated, 'a cyber-operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention' (Egan 2017). Australia, referencing the UK position, states that 'the use by a hostile State of cyber operations to manipulate the electoral system to alter the results of an election in another State (…) would constitute a violation of the principle of non-intervention' (Commonwealth of Australia 2020). Lastly, the G7, in 2017, expressed their increasing concern 'about cyber-enabled interference in democratic political processes' (G7 2017) and reiterated their concern in 2018 in the Charlevoix Commitment on Defending Democracy from Foreign Threats (see Broeders 2021, 8).

In July 2021, the official compendium of state positions on international law in cyberspace – originally intended to be annexed the UN GGE consensus report – was published (UNGA 2021c). 11 out of the 15 state contributions – including some countries mentioned above – make some reference to election interference in relation to breaches of sovereignty or the rule of non-intervention. Many of these are cautious and amended by the notion that much will depend on a 'case by case assessment' to determine whether there is a breach of international law and/or if the level of coercion is reached. Two state contributions stand out by explicitly flagging 'new terrain'. Norway states that '(…) manipulating election systems or unduly influencing public opinion through the dissemination of confidential information obtained through cyber operations ('hack and leak'), would be in violation of the prohibition of intervention' (UNGA 2021c, 69). In addition to calling out 'hack-and-leak' operations, Norway also stresses that states can be held responsible for election interference emanating from their territory based on the principle of due diligence (Ibid., 72). Switzerland – hiding a little behind the statement that 'the debate on sovereignty includes aspects such as … ' – flags information operations and the role of intelligence agencies as possible violations of the principle of non-intervention: '(…) situations in which a state has sought to influence, disrupt or delay democratic decision-making processes in another state through the coordinated use of legal and illegal methods in cyberspace e.g. propaganda, disinformation and covert actions by intelligence services' (UN GA 2021c, 87). In addition to more states placing election interference in the light of international law, some states are also cautiously beginning to be more specific.

In June 2018, the Global Commission on the Stability of Cyberspace proposed a norm for the protection of election infrastructure: 'State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites' (GCSC 2018). In November 2018, the Paris Call for

Trust and Security in Cyberspace – now signed by 79 states, including all EU member states, but not legally binding – addressed the issue of election interference. Specifically, the document calls on its signatories to cooperate to '(s)trengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities'. This norm addresses 'election processes', which could be interpreted as more than just the technical election infrastructure, but does so only in light of capacity building, thus avoiding a direct legal or normative condemnation other than calling the activities 'malign' and 'malicious'. Until 2021, the UN GGE consensus reports do not mention election interference, but the 2015 report did contain a non-binding norm that critical infrastructures should not be digitally attacked during peacetime (UNGA 2015, [article 13(f)]). Some countries, like the US, have since defined elections as critical infrastructure and, by doing so, have arguably moved them under the protection of the 2015 UN GGE norm (CISA 2019). Some countries, like the Netherlands (2020b) and Australia (2019) aimed to move forward on this issue in the 2021 rounds of the UN GGE and the OEWG (see Broeders [2021] for a detailed analysis).

The 2021 UN GGE and OEWG consensus reports are oddly complementary when it comes to the issue of election interference. In both reports, the issue is addressed only in the context of (technical) election infrastructure, shying away from information operations and hack-and-leak operations. In the OEWG report, election interference ('malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes') is mentioned only in the threats section, as the accompanying norm was deleted in the later drafts (UN GA 2021a, 4). In contrast, the UN GGE report has no mention of the issue in the threats section but does have one in the norms section under the norms on the protection of critical infrastructure, highlighting 'electoral processes' as a critical infrastructure (UN GA 2021b, 13). Three things can be taken from these recent views and comments. Firstly, states have increasingly become more explicit in flagging election interference as a problem of international law. They are mostly Western states, and the reference is exclusively to sovereignty and/or the principle of non-intervention. Iran recently also subscribed to this interpretation (Roguski 2020d). Secondly, states differ in the focus of their comments with some highlighting (technical) election infrastructure and some broadening it to election processes. Recently, some states have become a little more explicit in naming specific behaviour in relation to election interference that may be seen as a violation (hack-and-leak operations) but most states have issued rather general statements. Thirdly, the number of states or other actors that have mentioned or addressed the problem of election interference through covert information operations is very limited. This type of foreign digital interference is hardly addressed in legal and normative language yet, although the 2021 UN GGE report does state that 'the Group notes a worrying increase in States' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State' (UN GA 2021b, 7). The issue is making its way into the UN conversation and may reappear in the new OEWG deliberations.

5.3. Legal obstacles and possible ways forward

The threshold for *declaratory* policy seems to be lowering; states are preparing the ground to call out election interference in terms of international law. However, the legal details behind such a statement still need to be addressed. Moreover, to move forward, states may have to re-interpret some elements of the legal learnings on non-intervention to (re)fit both the problem (election interference) and the domain (cyberspace). Or, as Kilovaty puts it, if states hope to address these issues, it will take 'a new layer of legal subtlety' (2018, 152).

Most legal scholars see non-intervention as the most promising way forward, although some issues need to be addressed. States are generally held to be in breach of the principle of non-intervention when two cumulative conditions are met: (1) the action constitutes a *coercive* interference, (2) into the *domaine réservé* of a state, i.e. into the matters on which each state is permitted, by the principle of state sovereignty, to decide freely (Roguski 2020a). These conditions are not a natural fit with election interference, but neither is it impossible to argue the case. The first hurdle, arguing that elections are part of the *domaine réservé* of the state, seems attainable as legal scholars argue that the right of every state to choose its political system without interference is a core part of customary international law, and therefore that elections are part of the internal affairs of states (Schmitt 2018, 49 [if coercion requirement can be satisfied]; Roguski 2020a, 7). Some authors (see Ohlin [2018] and Tsagourias [2020]), discuss the possibility of making the violation of non-intervention more layered in a legal sense by connecting it to the principle of self-determination, i.e. 'the idea that peoples have a right to select their own political destiny, a process that in democratic societies is actualised through the electoral process' (Ohlin 2018, 3). Ohlin (2020, 103–104) argues that self-determination is legally protected by international law as a collective right in itself and therefore does not even have to be folded into the principle of non-intervention to provide protection for elections. Using the principle of self-determination to ground election interference – in itself or as a violation of non-intervention – makes for a strong case that states should be able to defend.

The bigger bone of contention is the condition of *coercive* interference. Election interference falls short of the fairly high threshold that most states require for coercion – even though the precise scope of coercion in cyberspace is generally unclear (Roguski 2020a, 6–7). Kilovaty (2018, 167) therefore poses the crucial and controversial question of 'whether coercion is still a reasonable standard to use in determining the lawfulness of states' actions in cyberspace'. He suggests that in cases of 'technically non-coercive but highly disruptive cyber-attacks' the norm against intervention should be considered violated 'when the attack causes 'disruption' rather than [the] outdated notion of 'coercion'' (169). In the case of attacks on election infrastructure, the threshold for non-intervention is more likely to breached using a standard of disruption rather than coercion.

In contrast, influence operations on social media are much harder to bring into the international legal fold. Not all relevant actors are state agencies, which increases the (im)plausible deniability (Cormac and Aldrich 2018) for the perpetrator and the burden of proof for the victim state. Schmitt, for example, argues that even though US intelligence attributed the IRA trolling to Russia with confidence, it did not do so in a legal sense (2018, 63). Tying non-state actors to their political overlords in a conclusive legal way requires high standards of proof about state control over non-state actors (Maurer 2016, 393–399). However, even though information operations are hard to link with coercion, and evidentiary standards for proxies are high, they will likely become a permanent fixture of low-level cyber conflict in years to come. Disinformation (campaigns) may 'pose some serious conceptual challenges to what is considered prohibitive intervention' (Kilovaty 2018, 178).

The best legal argument to bring disinformation into the equation is linked to self-determination. It is the covert impersonation of Americans – to increase the political effect of trolling – that legal scholars pick up on in the context of self-determination. If self-determination is the 'right of a people to choose its own political destiny' then it matters who the people are. Covert impersonation may create a legal problem, as Ohlin (2018, 13) argues, 'Once outsiders insert themselves into that process, while pretending to be insiders, the election becomes a function of other-determination rather than self-determination'. To him, 'the covert nature of the election interference was crucial to its illegality as a violation of the principle of self-determination' (ibid 13).

6. NotPetya

6.1. Possible triggers for the violation for norms, principles and law

NotPetya was a destructive malware[28] attack that primarily targeted Ukraine in June 2017, causing indiscriminate network damages to its hospitals, central bank, airports and state-owned power companies, as well as to private businesses and systems. Using the EternalBlue exploit, the malware masqueraded as ransomware of the Petya family, but ultimately had a destructive and political goal.[29] Through the encryption of computers' master boot records, NotPetya caused the impairment of machines due to the inability of the operative system to launch.[30] While victims were prompted with a ransom request, payments yielded no results as no key ever existed. The 'fake' ransomware was distributed through the Ukrainian tax accounting MeDoc software, extensively used by both public and private organisations across the country. Once launched, the cyberattack quickly spread and also shut down operations beyond Ukrainian networks and reached systems in 64 other countries. With total damages estimated by the White House to be over US$10 billion, NotPetya has been considered 'the most devastating cyberattack in history' (Greenberg 2018).

The NotPetya case gives rise to a number of debates related to the applicability of international law. The triggers for a potential violation of law and norms are represented by ransomware's indiscriminate nature, the damage caused to Ukrainian critical infrastructures, and the attackers' loss of control over the malware's spread once it had been set in motion. The spread and magnitude of the attack prompted immediate responses, with Ukraine's official attribution coming soon after the incident. Similar to the Iranian response to Stuxnet, national authorities initially downplayed the incident stating that, despite the panicked mood, 'the miscreants failed to cause significant harm'. In the same interview, Valentyn Petrov, head of the information security service at Ukraine's National Security and Defense Council, referred to the timing of the cyberattack – the eve of the country's Constitution Day – to infer its political motivation and Russia's responsibility (Kyiv Post 2017). Several other countries – Australia, Canada, Denmark, Estonia, Lithuania, the United Kingdom and the United States – followed hot on the heels of Ukrainian attribution and immediately released a coordinated response condemning the attack and attributing it to the Russian Federation. Amongst these, only Estonia mentioned international law, by calling on states to act 'responsibly and follow the rules of international cooperation and the norms of international law that apply in cyberspace' (MFA Estonia 2018). In 2019, two years after the attack, the EU Council also condemned the attack and referred to the UN GGE 2013 and 2015 reports specifying that international law's principles apply to cyberspace (Council of the European Union 2018). However, the EU Council's statement similarly failed to indicate which specific principles of international law had been violated.

While a fraction of the public attribution statements made a somewhat *implicit* reference to relevant principles of international law and normative views, these only considered Ukraine as an affected country. For example, the United Kingdom (United Kingdom's Foreign, Commonwealth & Development Office. 2018) – which views sovereignty as a political principle rather than as rule – asserted that 'the attack showed a continued disregard for Ukrainian sovereignty'. As noted by Moynihan, none of the statements referred to the violation of the territorial sovereignty of other countries that had been affected by the attack (2019, 35). Furthermore, the United States' attribution statement declared that the attack would be 'met with international consequences' but provided no further explanation on the nature and extent of these consequences at that time (White House 2018). Following public attribution, the United States Treasury imposed sanctions on individual officials of the GRU, pointing at their responsibility for both NotPetya and 2016s US election interference.[31]

6.2. New lines of legal or normative significance?

Similar to the attack against the Ukrainian power grid, the case of NotPetya can be considered in the context of an armed conflict between Russia and Ukraine (see, e.g. Schmitt and Biller [2017]). However, as NotPetya affected many other states beyond Ukraine, the incident can relate to the applicability of both wartime and peacetime norms and legislation.

6.2.1. Notpetya in the context of wartime

If we consider the case in the context of the Russia-Ukraine armed conflict, NotPetya raises the question of the applicability of IHL, specifically Article 49 of the Additional Protocol I. While there is no unanimous position – among scholars (Schmitt 2017b; ICRC 2019, 7) and states – on whether indiscriminate malware and ransomware attacks constitute an 'act of violence against the adversary, whether in offence or in defense', NotPetya could potentially fall within the scope of Article 49, when considering recent interpretations of IHL. For example, the official French interpretation would include such cyber operations, because they render the systems unable to 'provide the service for which they were implemented, whether temporarily or permanently, reversibly or not' (French Ministry of the Armies 2019, 13).

If NotPetya is considered to fit the definition of attack as provided by Article 49, the next question is whether automated cyber operations violate principles of distinction and/or the prohibition of indiscriminate attacks, codified respectively in Articles 48, 51 (2), 52(2) and 51(4) of the Additional Protocol I. Having targeted media organisations, banks and healthcare centres, NotPetya can be considered a violation of the principle of distinction insofar as civilian infrastructures were targeted *intentionally* (conform Kaminska, Broeders, and Cristiano 2021). Similarly, it can also constitute a violation of the prohibition of indiscriminate attacks as no effort was made by the perpetrator to distinguish between lawful targets and protected ones. With its effects going beyond Ukraine and targeting neutral states' infrastructures, NotPetya could potentially constitute a violation of the law of neutrality regulating international armed conflicts (Schmitt and Biller 2017; Kaminska, Broeders, and Cristiano 2021).

Further to the debates on cyber operations carried out in wartime, in January 2019, the NotPetya case featured an interesting development. When the food brand Mondelez claimed insurance compensation for part of the US$100 million spent on recovery from damages caused by NotPetya, the insurance company Zurich refused to settle the payment by referring to the war exclusion clause in the insurance contract.[32] Through this decision, Zurich acted upon the fact that various states attributed the cyberattack to Russia and a presumption that the attack should be considered in a context of war (Ferland 2019). The litigation case that is still ongoing in courts across the United States and the UK adds complexity to the legal interpretations of the use of cyber in hybrid times (Satariano and Perlroth 2019).

It is highly unlikely, however, that the outcome of the Zurich court case alone will constitute a relevant piece of jurisprudence regarding the applicability of international humanitarian law to cyber operations. While the court must decide whether the war clause applies, this decision will not answer the questions of *whether* and *how* international humanitarian law applies to the attack itself. Nevertheless, the court decision might provide an interesting angle for the analysis of the effects of public attributions of the attacks. While war exclusion clauses are nothing new in insurance policies, the future ruling on the Zurich insurance case would be unprecedented in the field of cyber insurance since the argument on war exclusion is based on the public attribution of the attacks to Russia made collectively by states.

6.2.2. Notpetya in the context of peacetime

As the effects of NotPetya went far beyond Ukrainian borders, it is essential to consider the extent to which international law, and the most recent non-binding normative frameworks, can be applied to state-sponsored automated attacks launched in peacetime. NotPetya raises the question of whether the attack constitutes a breach of sovereignty of both Ukraine and other affected countries, and/or a violation of the principle of non-intervention. While scholars point to the possibility that attacks like NotPetya violate sovereignty, diverging state positions on this issue – discussed above – make such application less straightforward (Cyber toolkit, scenario 14 2020; Moynihan 2019). The question of whether the NotPetya attack violated the principle of non-intervention – coercive interference into the *domaine réservé* of a state – is problematic.

As discussed earlier in this article, the condition of coercive interference in cyberspace lacks clarity and is being debated (Roguski 2020a, 7–8) as international law provides no definition of coercion and no guidance on what constitutes coercion in cyberspace (Kilovaty 2018, 168). Roguski (2020a, 8) highlights that some of the national interpretations construct the concept of coercion 'through its effects on the free exercise of the sovereign will of the State', which can take the form of depriving the state from exercising its sovereign powers. Even though NotPetya targeted the networks of Ukrainian public ministries, potentially affecting the country's *domaine réservé* (Schmitt and Biller 2017), it is not entirely clear whether this could meet the criteria of preventing the Ukrainian government from exercising its sovereign will. However, NotPetya could certainly cross the threshold of ‘disruption’ suggested by Kilovaty (2018, 169) as an alternative to the ‘outdated notion of coercion’.

In the absence of a unanimous position on the applicability of international law to indiscriminate cyberattacks, efforts to develop non-binding norms slowly move in the direction of acknowledging and addressing the problem of automated cyberattacks. Recent non-binding norms – part of initiatives like the 2018 Paris Call for Trust and Security in Cyberspace and the 2019 report of Global Commission on the Stability of Cyberspace – provide some elements of normative clarity. In particular, the Paris Call explicitly acknowledges the emergence of ‘malicious cyber activities in peacetime’ that are ‘threatening or resulting in significant, indiscriminate or systemic harm to individuals and critical infrastructure’ and welcomes ‘calls for their improved protection’. As the malware targeted end users, caused significant harm in other countries and has an indiscriminate nature, it could provide a normative benchmark for those states that were not at war with Ukraine. The same applies for norm 4 of the Global Commission on the Stability of Cyberspace that covers automated attacks of large scale by asserting that ‘state and non-state actors should not commandeer the general public’s ICT resources for use as botnets or for similar purposes.’ This norm seems to cover exclusively attacks committed with the use of botnets and thus it is unclear whether other automated attacks like NotPetya could fall under the scope of the ‘similar purposes’ clause.

6.3. Legal obstacles and possible ways forward

Due to its technical characteristics, the NotPetya attack ultimately points at normative and legislative vacua for addressing automated cyberattacks. The fact that collective public attributions raised the issue of sovereignty serves as an indicator that this is one of the routes that states could pursue in the future. Scholars seem to see sovereignty as the most promising route to tackle automated attacks as well – for example, the Cyberlaw toolkit, that considers ransomware attack as one of the possible scenarios, suggests that, while it is unlikely that a ransomware attack will trigger the application of the rules related to the use of force and non-intervention, such an attack could amount to the breach of the obligation to respect sovereignty (“Scenario 14” 2020).

However, to be considered such a violation, ransomware attacks have to result in severe disruption and loss of functionality, for example, when they disrupt the work of medical offices, municipal services, or interfere ‘with data or services that are necessary for the exercise of inherently governmental functions’ (“Scenario 14” 2020).[33] However, as Moynihan (2019) notes, the problem with pursuing the application of the violation of sovereignty rule in case of indiscriminate automated attacks, is the limits of expansion of this principle: would such attacks violate the sovereignty of *all* the states affected?

With regards to normative developments, the issue of states reverting to automated cyberattacks has been substantially ignored until now. The final reports of the most recent iterations of the OEWG and GGE (2021) make no mention of the issue of automation (or autonomy). A reference to automation as a ‘specific concern’ was however present in the OEWG’s second ‘pre-draft’ of the final report (2020b, 4) but was edited out of the final report as it did not carry consensus. It has been included in the OEWG Chair’s Summary: ‘pursuit of increasing automation and autonomy in ICT operations was put forward as a specific concern, as were actions that could lead to the reduction or disruption of connectivity, unintended escalation or effects that negatively impact third parties' (UNGA 2021d, 2). The issue is therefore likely to resurface in the 2021–2025 round of the OEWG that has just started up. Such efforts are important as they can shed light on the applicability of international law to automated attacks like NotPetya. While the principle of sovereignty seems to be the most applicable to such situations, the fact that the state has very little, or no, control over the distribution of automated attacks once the attack is launched, means that clarification on the applicability of international law in such situations should take these characteristics of particular attacks into consideration. This argument was also highlighted during the ongoing OEWG negotiations: for example, the Netherlands' comments assert that adherence to the norms of responsible behaviour becomes problematic as such automated operations can go outside of the control of those who launch them (Kingdom of the Netherlands 2020c, 2).

7. Conclusion: inch by inch, rather than in leaps

The aim of this article was to see whether recent efforts to formulate and interpret legal and/or normative lines of significance to judge the (un)lawfulness and (il)legitimacy of cyber operations could lead to a different legal and normative evaluation of a number of notorious cyber operations that occurred between 2010 and 2017. Would current thinking have made a difference in the way states – and other actors in the normative field – could (and would) judge these attacks should they happen today? Do the new norms and interpretations of laws and norms that states and other actors have formulated make a difference in calling out cyber operations? Do changes in the political context change the incentive structures for states to attribute cyber operations to states, invoke international law, and to impose consequences? In this article we have looked at a diverse range of five state-led or sponsored cyber operations that took place between 2010 and 2017. Ranging from digital espionage – via election interference – to sabotage, they vary in the (kind of) damage they have done and the possible tensions with (interpretations of) international law and norms of state behaviour.

Nearly 12 years – Stuxnet dates back to 2010 – do seem to have made a difference, even though legal and normative thinking in cyberspace proceeds inch by inch, rather than in leaps. The past 11 years do give rise to the idea that some of the cases would have been dealt with differently today. Given the increasing use of language relating to violation of sovereignty in recent public attributions, and the damage done to critical infrastructure, Stuxnet would likely be called out as a violation of sovereignty today. The Belgacom hack would probably still be accepted as a lawful form of intelligence gathering in a legal sense, but the prominence of intelligence agencies in cyberspace has given rise to new thinking about peacetime cyberespionage. Academics especially are moving beyond the blanket statement that international law does not forbid espionage and are exploring a more fine-grained analysis of what is and isn't allowed.

In doing so, some are moving away from a damage threshold towards an assessment of the context and purpose of espionage to evaluate lawfulness. More recently, a risk-based approach seems to be gaining traction. The attack on Ukraine's power grid was 'plagued' by the question of whether it took place in wartime or in peacetime and by a lack of a credible attribution. Given the rise in public attributions – often for less impactful cyber operations – one might expect a public attribution coalition to assign responsibility should it happen today. The coalition that attributed the NotPetya attack just a few years later is an indication. If a power grid attack happened during wartime, as an operation against civilian infrastructure, it could potentially constitute a violation of IHL's principle of distinction that protects civilian targets against attacks. In peacetime it would now probably qualify as a violation of sovereignty and/or a violation of the principle of non-intervention. Moreover, at the normative level, the protection of critical infrastructure has been put front and centre since the 2015 GGE report, and in the 2021 OEWG report and UN GGE report, much has been done to strengthen the articles on critical infrastructure protection. The OEWG report even states that attacks on critical infrastructure '(…) could pose a threat not only to security but also to State sovereignty' (UNGA 2021a, 4). The emphasis by many states that the 2021 GGE report should add a 'layer of understanding' to the 2015 norms, rather than create new norms, did mean that things like election interference were narrowed down to interference with election infrastructure instead of the wider category of election processes.

The relative lack of consequences for cyber operations has been one of the drivers behind public attribution coalitions and for the few inches that states have moved forward in calling out, or preparing the ground to call out, cyberattacks in terms of international law. The interference with the US elections is a case in point – it was attributed to Russia but met with a response of limited consequences. Some states are becoming more explicit in their view that election interference should be regarded as a violation of the principle of non-intervention, and scholars are arguing the case that the violation of the non-intervention principle should be grounded in the principle of self-determination. Some argue that the latter principle is enough in itself to challenge election interference. Thus, the groundwork is being laid to call out future election interference more forcefully. The NotPetya case already reveals a major difference from 2010 because of the coordinated multi-state attribution, although the attack was still met with very limited consequences. The attacks also resonate with concerns about automated, indiscriminate attacks that have surfaced in the OEWG negotiations and in other fora for norms.

On a more abstract level, a number of conclusions about, and evaluations of, recent changes in the political context and in legal and normative thinking can be drawn. In the last couple of years we have seen an increase in public state attributions, including an increase in collective and coordinated attributions, although these are still mostly a Western affair. This is noteworthy because: (a) states are attributing cyberattacks that are much more modest in scope than some of the attacks of the past, suggesting that more severe attacks are more likely to be called out publicly should they happen today; and (b) attribution is a necessary, but not sufficient, condition for states to invoke international law in response to an attack.

States rarely attribute with reference to international law, although blanket references – 'this attack is in breach of international law' – are on the rise and, in some cases, there is even reference to individual principles of international law that are breached. In the latter case, these are almost invariably the principle of sovereignty and/or the principle of non-intervention. The number of states that have issued some statement or document on *how* states see the application of international law in cyberspace – beyond the position *that* international law applies in cyberspace – is growing. The recently published official compendium of state visions on international law in cyberspace (UNGA 2021c) adds some more granularity, but also highlights that major (cyber) powers, such as China, have not put out their vision yet. In most statements, sovereignty and non-intervention are again the principles of international law that are dealt with in more, albeit still modest, detail. However, given the fact that states will differ in their interpretation of the law – with diverging interpretations of sovereignty as a major example – this process has elements of legal clarification and convergence as well as fragmentation. States' hesitancy to take detailed positions on these legal issues may also be hampered by the fact that many cyber operations are foreign intelligence operations or, even when they are not, they are executed by intelligence agencies. As espionage is largely unaddressed by international law and states are also eager to avoid binding their own hands when it comes to intelligence gathering, many states are cautious about drawing lines in the sand. However, pressure from home audiences to do so is increasing (Devanny, Martin, and Stevens 2021).

Non-binding norms, such as the GGE norms for responsible state behaviour and other documents, such as the Paris call, have not yet featured much in state attributions or other statements. However, new 'sources of norms' do inform some of the input by states into state-led processes such as the OEWG and the UN GGE, as evidenced by some of the language on 'the public core of the internet', election interference and threats against the healthcare sector in the 2021 UN consensus reports.

Many scholars – especially international law scholars – have indicated with some impatience that states need to step up to the plate to indicate exactly how cyberattacks violate specific articles of international law. This need stems both from the perspective of the role that international law can play in contributing to international stability, as well as from the perspective of the development of the field of international law itself. Only state practice can create customary law, but in the words of Ohlin (2018), scholars should not confuse the 'identification of the legal rule with the application of that legal rule' meaning that once 'the legal rule is established as a valid rule of law, one can then apply it in genuinely novel situations.'[34] Scholars and states are at least to some extent in the same position; creative thinking is needed to increase the granularity of the legal and normative analysis. States are taking small steps towards creating state practice.

In the current climate, some of the cyber operations analysed would almost certainly not go without a public attribution if they happened today and, in the case of some of the more damaging attacks (Stuxnet, the Ukrainian power grid and NotPetya), these would now be more likely to be called out in terms of international law and norms of state behaviour. Recent public attributions of the SolarWinds operation indicate that even states' patience with high-level cyberespionage cases becomes more limited. If the website defacements in Georgia are condemned as a violation of sovereignty in 2020, it would be hard to call out a cyberattack on the power grid of a sovereign state as anything less, should it occur today. In that sense, states are slowly raising the stakes for attribution and the legal and normative lines of significance to call out irresponsible state behaviour in cyberspace. Public attribution thus paves the way for international law to play a role, but only states can make it a reality.

Notes

1. The Tallinn Manual (Schmitt 2013) and the Tallinn Manual 2.0 (Schmitt 2017a) are both non-legally binding scholarly works by distinguished international law academics and

practitioners intended to provide an objective restatement of international law as applied in the cyber context. Work is currently underway on a third, 3.0, edition of the manual. See https://ccdcoe.org/research/tallinn-manual/.

2. Charter of Trust <https://www.charteroftrust.com/>.
3. See, e.g., Microsoft, 'A Digital Geneva Convention to protect cyberspace' (Microsoft Policy Papers) <https://www.microsoft.com/en-us/cybersecurity/content-hub/a-digital-geneva-convention-to-protect-cyberspace>; Microsoft, 'International Cybersecurity Norms' (Microsoft Policy Papers) <https://www.microsoft.com/en-us/cybersecurity/content-hub/international-cybersecurity-norms-part-2>; Cyber Tech Accord <https://cybertechaccord.org/>. For an analysis of Microsoft initiatives, see Gorwa and Perez (2020) and Hurel and Lobato (2020).
4. Global Commission on the Stability of Cyberspace <https://cyberstability.org/>.
5. For example, at the time of writing, over 20 countries and the EU, as an international organisation, have issued statements on the cyber-attacks on Georgia in October 2019.
6. United Nations Office for Disarmament Affairs, 'Open-ended Working Group' <https://www.un.org/disarmament/open-ended-working-group/>.
7. Further research conducted by Symantec in 2013 indicated that the worm had been circulating since 2005 (conform McDonald et al. 2013).
8. For a detailed account of the Stuxnet's background and operational phase, please see Zetter (2014) and Langner (2013). On Israel's cyber capabilities, see Cristiano (2020a).
9. Because of this, the spread of Stuxnet beyond the initially targeted computer systems was extremely limited and only lead to minor damages in India, Indonesia, China, Azerbaijan, South Korea, Malaysia, the United States, the United Kingdom, Australia, Finland and Germany.
10. As argued by Zetter (2014) in *Countdown to Zero Day*, Iranian authorities had noticed damages to the nuclear centrifuges already in 2009 but failed to detect the cyberattack.
11. David Sanger published further details on the Israel-US partnership ahead of Stuxnet in his 2012 book *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*.
12. Buchan (2012). On this issue, Buchan (2012, 217) writes that '(a)t first, it was generally accepted that armed force required the use of a weapon that produced kinetic force', but then continues, '(a)ppreciating that Article 2(4) is an effects-based prohibition, determining whether the attack against Iran amounted to an unlawful use of force is problematic because the exact impact of the Stuxnet virus has never been concretely identified' (220).
13. On the other hand, and in line with Buchan (2012), many argue that that Article 2(4) shall be considered effects-based rather than weapon-based, this way overcoming the debated equation between Stuxnet and a kinetic weapon; conform Sharp (1999, 140), Keber and Roguski (2011), and Roscini (2014, 49–52). The characterisation of Stuxnet as a weapon has also triggered a polarising academic debate on whether it can be considered a 'perfect weapon' or not (see Sanger [2018] and Rid [2018]), and also on how it exposes the limits of cyberwarfare (Lindsay 2013).
14. The International Court of Justice specifies the meaning of the category 'armed attack' as 'the most grave form of the use of force' (ICJ 1986, paragraph 191). In other words, 'the result is a normative schema in which all armed attacks are uses of force, but not all uses of force are armed attacks' (Schmitt 2012, 286).
15. On the broader geopolitical polarisation at the OEWG, see Cristiano (2020b).
16. The Belgian government is the majority owner of Belgacom.
17. UN GGE (2015), Norm (d).
18. See also Protocol (No 21) on the Position of the United Kingdom and Ireland in Respect of the Area of Freedom, Security and Justice [2016] OJ C202/295.
19. See for example, Article 2 of the Council of Europe Convention on Mutual Assistance in Criminal Matters.
20. During a workshop organised by The Hague Programme for Cyber Norms, 10 of 15 intelligence experts labelled the Belgacom hack as a contested form of espionage; see Broeders, Boeke, and Georgieva (2019, 2); see also Lubin (2020, 197) and Navarrete and Buchan (2019, 898–901).

21. See criticism on this paper in Schmitt and Vihul (2017b).
22. Russia has been accused by Ukrainian authorities of launching cyberattacks against power companies; see Newsweek (2016).
23. See also in Russian, 'США помогут расследовать кибератаку на энергосистему Украины' (12 January 2016) <https://www.rbc.ua/rus/lnews/ministerstvo-natsbezopasnosti-ssha-pomozhet-1452630011.html>.
24. Acquired by FireEye in January 2015.
25. Global Commission on the Stability of Cyberspace <https://cyberstability.org/>.
26. Kilovaty calls this 'Doxfare', in a play on words on the concept of lawfare.
27. Including the additional measures taken at the time of the public attribution of the Solar-Winds operation in April 2021. See https://home.treasury.gov/news/press-releases/jy0126.
28. Taking into consideration that no ransom could be actually paid, we opted for defining Not-Petya as malware or 'fake ransomware'.
29. As the EternalBlue exploit has allegedly been developed by the NSA, and then leaked by the hacker group Shadow Broker, the case of NotPetya could be interpreted as a lack of due diligence of the United States. See e.g., NATO CCD COE (2017).
30. For an in-depth technical analysis of NotPetya, see Watson (2017).
31. Under the Countering America's Adversaries Through Sanctions Act (CAATSA) and the Executive Order (E.O.) 13694, 'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities', see US Department of the Treasury (2018).
32. See the document at: *Mondelez International Inc v Zurich American Insurance Company*, No. 2018L011008, 2018 WL 4941760 (Ill. Cir. Ct. Oct. 10, 2018) <https://www.databreachninja.com/wp-content/uploads/sites/63/2019/01/MONDELEZ-INTERNATIONAL-INC-Plaintiff-v-ZURICH-AMERICAN-INSURANCE-COMPANY-Defenda.pdf>.
33. It should be noted that, in practice, the disruption and loss of functionality, even if the incident interferes with functions such as medical services, does not always lead to claims of violation of sovereignty. For example, such incidents as Düsseldorf University Hospital services hack in September 2020 (BBC News 2020) which prevented the hospital from accepting emergency patients, haven't led to any such claims, despite the reports that investigation revealed that Russian hackers could have been behind the attack (Paganini 2020).
34. Although legal interventionism in cyberspace also has its limitations and pitfalls, see d'Aspremont (2016).

Acknowledgements:

This paper was first presented at the 2020 conference *Moving Forward: Fragmentation, Polarisation and Hybridity in Cyberspace*, organised by The Hague Programme for Cyber Norms, and benefited from the discussion there. The authors gratefully acknowledge the time spent, and constructive comments given, by Przemysław Roguski, Russell Buchan and François Delerue on earlier versions of this paper. Lastly, we would like to thank the anonymous reviewers and the editorial team of the *Journal of Cyber Policy* for their constructive comments.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported by Microsoft; Ministerie van Buitenlandse Zaken: [Grant Number The Hague Programme for Cyber Norms].

Notes on contributors

Dennis Broeders is full professor of Global Security and Technology and senior fellow of The Hague Program on International Cyber Security at the Institute of Security and Global Affairs of Leiden University

Els De Busser is Assistant Professor Cybersecurity Governance at the Institute of Security and Global Affairs of Leiden University and a fellow of The Hague Program on International Cyber Security.

Fabio Cristiano is a postdoctoral researcher in the Institute of Security and Global Affairs at Leiden University and a fellow of The Hague Program on International Cyber Security.

Tatiana Tropina is Assistant Professor Cybersecurity Governance at the Institute of Security and Global Affairs of Leiden University and a fellow of The Hague Program on International Cyber Security.

ORCID

Dennis Broeders http://orcid.org/0000-0002-8827-2814
Els de Busser http://orcid.org/0000-0002-7843-8833
Fabio Cristiano http://orcid.org/0000-0002-0951-9648
Tatiana Tropina http://orcid.org/0000-0001-7411-5060

References

Australian Mission to the United Nations. 2019. "Australian Paper – Open Ended Working Group on Developments in the Fields of Information and Telecommunications in the Context of International Security." September. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

Baezner, Marie. 2018. *Cyber and Information Warfare in the Ukrainian Conflict*. Zürich: Center for Security Studies, Cyber Defense Project.

BBC News. 2013a. "European Commission VP Neelie Kroes: Spying 'not acceptable at all'." *BBC*, July 1. https://www.bbc.com/news/av/world-europe-23129123/european-commission-vp-neelie-kroes-spying-not-acceptable-at-all.

BBC News. 2013b. "Merkel calls Obama about 'US spying on her phone'." *BBC*, October 23. https://www.bbc.com/news/world-us-canada-24647268.

BBC News. 2018. "How the Dutch foiled Russian 'cyber-attack' on OPCW." *BBC*, October 4. https://www.bbc.com/news/world-europe-45747472.

BBC News. 2020. "Police launch homicide inquiry after German hospital hack". *BBC*, September 18. https://www.bbc.com/news/technology-54204356.

Belgacom. 2013. "Belgacom takes actions related to IT security." Press release, *Belgacom*, September 16. https://web.archive.org/web/20131211170608/http://www.belgacom.com/be-en/newsdetail/ND_20130916_Belgacom.page.

Boeke, Sergei, and Dennis Broeders. 2018. "The Demilitarisation of Cyber Conflict." *Survival* 60 (6): 73–90. doi:10.1080/00396338.2018.1542804.

Brière, Chloé. 2020. "Brexit and its consequences for cooperation in criminal matters." *European Law Blog*, February 3. https://europeanlawblog.eu/2020/02/03/brexit-and-its-consequences-for-cooperation-in-criminal-matters/.

Broeders, Dennis. 2020. "Creating Consequences for Election Interference." *Directions. Cyber Digital Europe*, May 15. https://directionsblog.eu/creating-consequences-for-election-interference/.

Broeders, Dennis. 2021. "The (Im)possibilities of Addressing Election Interference and the Public Core of the Internet in the UN GGE and OEWG: a Mid-Process Assessment." *Journal of Cyber Policy* 6 (3): 277–297. doi:10.1080/23738871.2021.1916976.

Broeders, Dennis, Sergei Boeke, and Ilina Georgieva. 2019. *Foreign intelligence in the digital age. Navigating a state of 'unpeace'*. The Hague Program for Cyber Norms Policy Brief, September.

https://www.thehaguecybernorms.nl/research-and-publication-posts/foreign-intelligence-in-the-digital-age-navigating-a-state-of-unpeace.

Broeders, Dennis, and Fabio Cristiano. 2020. "Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road." In *Fragmenting the Internet: States' Policies in the Digital Arena*, edited by Samuele Dominioni and Fabio Rugge, 8–10. Milan: ISPI.

Brown, Gary D. 2011. "Why Iran Didn't Admit Stuxnet Was an Attack?" *Joint Force Quarterly* 63 (4): 70–73.

Buchan, Russell. 2012. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict & Security Law* 17 (2): 211–227.

Buchan, Russell. 2018. *Cyber Espionage and International Law*. Oxford: Hart Publishing.

Buchan, Russell. 2020. "When More is Less: The US Department of Defense's Statement on Cyberspace." *EJIL Talk!*, March 30. https://www.ejiltalk.org/when-more-is-less-the-department-of-defenses-statement-on-cyberspace/.

Call, Paris. 2018. "Paris Call for Trust and Security in Cyberspace." November 12. https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_cyber_cle443433-1.pdf.

CISA (Cybersecurity & Infrastructure Security Agency). 2016. "ICS Alert (IR-ALERT-H-16-056-01): Cyber-Attack Against Ukrainian Critical Infrastructure." *Cisa.gov,* February 25. https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01.

CISA (Cybersecurity & Infrastructure Security Agency). 2019. "Election Infrastructure Security." *Cisa.gov*, March 15. https://www.dhs.gov/cisa/election-security.

CISA (Cybersecurity & Infrastructure Security Agency). 2020. "NSA Releases Advisory on Sandworm Actors Exploiting an Exim Vulnerability." *Cisa.gov*, May 28. https://www.us-cert.gov/ncas/current-activity/2020/05/28/nsa-releases-advisory-sandworm-actors-exploiting-exim.

Commonwealth of Australia. 2020. Australia Non Paper: Case Studies on the Application of International Law in Cyberspace. February 5. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/australian-international-law-case-studies-final-5-february-2020.pdf.

Cormac, Rory, and Richard J. Aldrich. 2018. "Grey is the New Black: Covert Action and Implausible Deniability." *International Affairs* 94 (3): 477–494. doi:10.1093/ia/iiy067.

Corn, Gary P., and Robert Taylor. 2017. "Sovereignty in the Age of Cyber." *AJIL Unbound* 111: 207–212. doi:10.1017/aju.2017.57.

Council of the European Union. 2018. 7517/18, Council Conclusions on Malicious Cyber Activities – Approval. April 16. https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf.

Cristiano, Fabio. 2020a. "Israel: Cyber Warfare and Security as National Trademarks of International Legitimacy." In *Routledge Companion to Global Cyber-Security Strategy*, edited by S. N. Romaniuk, and M. Manjikian, 409–417. Basingstoke: Palgrave Macmillan.

Cristiano, Fabio. 2020b. "The Road Toward Agonistic Pluralism for International Cyber Norms." *NetPolitics*, July 6. https://www.cfr.org/blog/road-toward-agonistic-pluralism-international-cyber-norms.

d'Aspremont, Jean. 2016. "Cyber Operations and International Law: An Interventionist Legal Thought." *Journal of Conflict & Security Law* 21 (3): 575–593. doi:10.1093/jcsl/krw022.

Davis, Ian, and David Isenberg. 2003. "The long history of UN espionage." *The Guardian*, March 9. https://www.theguardian.com/world/2003/mar/09/iraq.unitednations.

De Busser, Els. 2017. "Recommandation 13 (d)." In *Voluntary, Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology: A Commentary*, edited by Eneken Tikk, 77–94. New York: UNODA.

De Morgen. 2018. "Nieuwe aanwijzingen dat Britse geheime dienst achter hacking Belgacom zat." *De Morgen*, September 20. https://www.demorgen.be/nieuws/nieuwe-aanwijzingen-dat-britse-geheime-dienst-achter-hacking-belgacom-zat~b8faaf63/.

De Standaard. 2013. "Regering zal gepaste stappen ondernemen bij cyberspionage." *De Standaard,* September 16. https://www.standaard.be/cnt/dmf20130916_00743574.

Delerue, François. 2020. *Cyber Operations and International Law*. Cambridge: Cambridge University Press.

Denning, Dorothy E. 2012. "Stuxnet: What Has Changed?" *Future Internet* 4 (3): 672–687. doi:10.3390/fi4030672.

Der Spiegel International. 2013. “Britain’s GCHQ Hacked Belgian Telecoms Firm.” *Der Spiegel International*, September 20. https://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

Devanny, Joe, Ciaran Martin, and Tim Stevens. 2021. “On the Strategic Consequences of Digital Espionage.” *Journal of Cyber Policy* 6 (3): 429–450. doi:10.1080/23738871.2021.2000628.

E-ISAC. 2016. TLP: White. Analysis of the Cyber Attack on the Ukrainian Power Grid. Defense Use Case. March 18. https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

EDPS (European Data Protection Supervisor). 2017. Assessing the Necessity of Measures That Limit the Fundamental Right to the Protection of Personal Data: A Toolkit, April 11.

Efrony, Dan, and Yuval Shany. 2018. “A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice.” *American Journal of International Law* 112 (4): 583–657. doi:10.1017/ajil.2018.86.

Egan, Brian J. 2017. “International Law and Stability in Cyberspace.” *Berkeley Journal of International Law* 35 (1): 169–180.

Egloff, Florian J. 2020. “Contested Public Attributions of Cyber Incidents and the Role of Academia.” *Contemporary Security Policy* 41 (1): 55–81. doi:10.1080/13523260.2019.1677324.

Eichensehr, Kristen. 2020. “The Law & Politics of Cyberattack Attribution.” *UCLA Law Review* 67: 522–598.

Eichensehr, Kristen. 2021. “SolarWinds: Accountability, Attribution and Advancing the Ball.” *Just Security*, April 16. https://www.justsecurity.org/75779/solarwinds-accountability-attribution-and-advancing-the-ball/.

European Parliament. 2013. “Committee on Civil Liberties, Justice and Home Affairs Meeting.” *Europarl*, October 3. https://www.europarl.europa.eu/ep-live/en/committees/video?event=20131003-1500-COMMITTEE-LIBE.

Falliere, Nicolas, Liam O Murchu, and Eric Chien. 2010. *W32.Stuxnet Dossier*. Symantec Security Response, November. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf.

Farwell, James P., and Rafal Rohozinski. 2011. “Stuxnet and the Future of Cyber War.” *Survival* 53 (1): 23–40. doi:10.1080/00396338.2011.555586.

Ferland, Justine. 2019. “Cyber Insurance – What Coverage in Case of an Alleged Act of War? Questions Raised by the Mondelez v. Zurich Case.” *Computer Law & Security Review* 35 (4): 369–376. doi:10.1016/j.clsr.2019.06.003.

Fidler, David P. 2011. “Was Stuxnet an Act of War? Decoding a Cyberattack.” *IEEE Security & Privacy* 9 (4): 56–59. doi:10.1109/MSP.2011.96.

FireEye. 2016. Cyber Attacks on the Ukrainian Grid: What You Should Now. FireEye Industry Intelligence Report. https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf.

French Ministry of the Armies. 2019. *International Law Applied to Operations in Cyberspace*. https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf.

G7. “G7 Declaration on Responsible States Behavior in Cyberspace.”. 2017. April 11. https://www.mofa.go.jp/files/000246367.pdf.

Gallagher, Ryan. 2014. “The Inside Story of How British Spies Hacked Belgium’s Largest Telco.” *The Intercept*, December 13. https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/.

Gallagher, Ryan. 2018. “How U.K. Spies Hacked a European Ally and Got Away With It.” *The Intercept*, February 17. https://theintercept.com/2018/02/17/gchq-belgacom-investigation-europe-hack/.

GCSC (Global Commission on the Stability of Cyberspace). 2018. “Global Commission Urges Protecting Electoral Infrastructure.” *Cyberstability.org*, June 5. https://cyberstability.org/news/call-to-protect-electoral-infrastructure/.

Géry, Aude, and François Delerue. 2020. “A New UN Path to Cyber Stability.” *Directions – Cyber Digital Europe*, October 6. https://directionsblog.eu/a-new-un-path-to-cyber-stability/.

Gorwa, Robert, and Anton Perez. 2020. “Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft’s Cybersecurity Tech Accord.” In *Governing Cyberspace: Behavior, Power and Diplomacy*, edited by Dennis Broeders, and Bibi van den Berg, 263–284. London: Rowman & Littlefield International.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History." *WIRED*, August 22. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Hathaway, Melissa. 2017. "Getting beyond Norms: When Violating the Agreement Becomes Customary Practice." CIGI Papers No. 127, April.

Hern, Alex. 2016. "Ukrainian blackout caused by hackers that attacked media company, researchers say." *The Guardian*, January 7. https://www.theguardian.com/technology/2016/jan/07/ukrainian-blackout-hackers-attacked-media-company.

Hollis, Duncan B. 2020a. *Improving Transparency – International Law and State Cyber Operations: Fourth Report*. March 5, CJI/doc 603/20 rev. 1 corr. 1. http://www.oas.org/en/sla/iajc/docs/CJI_doc_603-20_rev1_corr1_eng.pdf.

Hollis, Duncan B. 2020b. *Improving Transparency – International Law and State Cyber Operations: Fifth Report*. August 7, CJI/doc. 615/20 rev. 1. http://www.oas.org/en/sla/iajc/docs/CJI-doc_615-20_rev1_ENG.pdf.

Hultquist, John. 2016. "Threat Research: Sandworm Team and the Ukrainian Power Authority Attacks." *FireEye Blog*, January 8. https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html.

Hurel, Louise Marie, and Luisa Cruz Lobato. 2020. "Cyber-Norms Entrepreneurship? Understanding Microsoft's Advocacy on Cybersecurity." In *Governing Cyberspace: Behavior, Power and Diplomacy*, edited by Dennis Broeders, and Bibi van den Berg, 285–313. London: Rowman & Littlefield International.

ICC. 2016. Report on Preliminary Examination Activities. https://www.icc-cpi.int/iccdocs/otp/161114-otp-rep-PE_ENG.pdf.

ICRC. 2019. "International Humanitarian Law and Cyber Operations During Armed Conflicts." ICRC position paper, November 28. https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

Islamic Republic of Iran. 2019. "Open-Ended Working Group on: Developments in the Field of Information and Telecommunications in the Context of International Security." Submission by the Islamic Republic of Iran, September. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/09/iran-submission-oewg-sep-2019.pdf.

Jamieson, Kathleen H. 2020. *Cyberwar: How Russian Hackers and Trolls Helped Elect a President: What We Don't, Can't and Do Know*. Oxford: Oxford University Press.

The Jerusalem Post. 2011. "IRNA: Stuxnet a product of US and Israel." *The Jerusalem Post*, April 16. https://www.jpost.com/breaking-news/irna-stuxnet-a-product-of-us-and-israel.

Jupillat, Nicolas. 2017. "From the Cuckoo's Egg to Global Surveillance: Cyber Espionage That Becomes Prohibited Intervention." *North Carolina Journal of International Law and Commercial Regulation* 42 (4): 933–988.

Kaminska, Monica, Dennis Broeders, and Fabio Cristiano. 2021. "Limiting Viral Spread: Automated Cyber Operations and the Principles of Distinction and Discrimination in the Grey Zone." In *13th International Conference on Cyber Conflict: 'Going Viral'*, edited by T. Jančárková, L. Lindström, G. Visky, and P. Zotz, 59–72. Tallinn: CCDCOE.

Keber, Tobias O., and Przemysław Roguski. 2011. "Ius ad bellum electronicum? Cyberangriffe im Lichte der UN-Charta und aktueller Staatenpraxis." *Archiv des Völkerrechts* 49 (4): 399–434. https://www.jstor.org/stable/41503401.

Kilovaty, Ido. 2014. "Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare." *National Security Law Brief* 5 (1): 91–124.

Kilovaty, Ido. 2018. "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponised Information." *Harvard National Security Journal* 9: 146–179.

Kingdom of the Netherlands, Government of the. 2020a. "Appendix: International Law in Cyberspace." https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/appendix-Internaional-law-in-cyberspace-kingdom-of-the-netherlands.pdf.

Kingdom of the Netherlands, Government of the. 2020b. "The Netherlands' Position Paper on the UN Open-ended Working Group 'on Developments in the Field of Information and

Telecommunications in the Context of International Security' and the UN Group of Governmental Experts 'on Advancing Responsible State Behavior in Cyberspace in the Context of International Security'." https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf.

Kingdom of the Netherlands, Government of the. 2020c. "The Kingdom of the Netherlands' Response to the Pre-Draft Report of the OEWG." https://front.un-arm.org/wp-content/uploads/2020/04/kingdom-of-the-netherlands-response-pre-draft-oewg.pdf.

Kovacs, Eduard. 2015. "Ukraine Accuses Russia of Hacking Power Companies." *Security Week*, December 30. https://www.securityweek.com/ukraine-accuses-russia-hacking-power-companies.

Kushner, David. 2013. "The Real Story of Stuxnet." *IEEE Spectrum*, February 26. https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet.

Langner, Ralph. 2013. To Kill a Centrifuge: A Technical Analysis of What Stuxnet's Creators Tried to Achieve. The Langner Group, November. https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf.

Lin, Herbert. 2012. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 6 (3): 46–70. https://www.jstor.org/stable/26267261.

Lindsay, Jon. 2013. "Stuxnet and the Limits of Cyber Warfare." *Security Studies* 22 (3): 365–404. doi:10.1080/09636412.2013.816122.

Lubin, Asaf. 2018. "Cyber Law and Espionage Law as Communicating Vessels." In *2018 10th International Conference on Cyber Conflict, CyCon X: Maximising Effects*, edited by T. Minárik, R. Jakschis, and L. Lindström, 203–226. Tallinn: NATO CCD COE Publications.

Lubin, Asaf. 2020. "The Liberty to Spy." *Harvard International Law Journal* 61 (1): 185–243.

Markoff, Michele. 2017. "Explanation of Position at the Conclusion of the 2016-2017 UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security." United States Mission to the United Nations, June 23. https://usun.usmission.gov/explanation-of-position-at-the-conclusion-of-the-2016-2017-un-group-of-governmental-experts-gge-on-developments-in-the-field-of-information-and-tele/.

Markoff, Michele, Paul Nicholas, Martha Finnemore, Duncan Hollis, and Tim Maurer. 2017. "Cyber Norms Revisited; International Cybersecurity and the Way Forward." Carnegie Endowment for International Peace, February 6. https://carnegieendowment.org/2017/02/06/cyber-norms-revisited-international-cybersecurity-and-way-forward-event-5490.

Marks, Joseph. 2017. "New International Cyber Rules Likely Off the Table for UN Experts Group." *Nextgov*, February 6. https://www.nextgov.com/cybersecurity/2017/02/new-international-cyber-rules-likely-table-un-experts-group/135193/.

Marquis-Boire, Morgan, Claudio Guarnieri, and Ryan Gallagher. 2014. "Secret Malware in European Union Attack Linked to U.S. and British Intelligence." *The Intercept*, November 24. https://theintercept.com/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/.

Maurer, Tim. 2016. "'Proxies' and Cyberspace." *Journal of Conflict and Security Law* 21 (3): 383–403.

McDonald, Geoff, Liam O Murchu, Stephen Doherty, and Eric Chien. 2013. *Stuxnet 0.5: The Missing Link*. Symantec Security Response, February 26. https://docs.broadcom.com/doc/stuxnet-missing-link-13-en.

McLellan, Charles. 2016. "How hackers attacked Ukraine's power grid: Implications for Industrial IoT security." *ZDNet*, March 4. https://www.zdnet.com/article/how-hackers-attacked-ukraines-power-grid-implications-for-industrial-iot-security/.

Merezhko, Oleksandr. 2018. "International Legal Aspects of Russia's War Against Ukraine in Eastern Ukraine." In *The Use of Force against Ukraine and International Law*, edited by S. Sayapin, and E. Tsybulenko, 111–121. The Hague: T.M.C. Asser Press.

MFA Estonia (Estonian Ministry of Foreign Affairs). 2018. "Foreign Minister Mikser condemns Russia for NotPetya attacks against Ukraine." February 15. https://vm.ee/ru/node/51114.

Minns, Jeanette, and Stephen Brown. 2015. "Germany spied on friends, allies and the Vatican." *Politico*, November 8. https://www.politico.eu/article/bnd-intelligence-germany-spied-on-friends-allies-and-the-vatican/.

Modderkolk, Huib. 2018. "Zo komen de Britten weg met de gigantische Belgacom-hack." *De Morgen*, February 17. https://www.demorgen.be/nieuws/zo-komen-de-britten-weg-met-de-gigantische-belgacom-hack~b934bccd/.

Moynihan, Harriet. 2019. "The Application of International Law to State Cyberattacks: Sovereignty and Nonintervention." Chatham House Research Paper. December 2019. https://www.chathamhouse.org/ publication/application-international-law-state-cyberattacks-sovereignty-and-non-intervention.

Mueller, R. S., III 2019. Report on the Investigation into Russian Interference in the 2016 Presidential Election (volume 1 of II). https://www.justice.gov/archives/sco/file/1373816/download.

Nakashidze, Giorgi. 2020. "Cyberattack against Georgia and International Response: emerging normative paradigm of 'responsible state behavior in cyberspace'?" *EJIL Talk!*, February 28. https://www.ejiltalk.org/cyberattack-against-georgia-and-international-response-emerging-normative-paradigm-of-responsible-state-behavior-in-cyberspace/.

Nakashima, Ellen. 2016. "Russian hackers suspected in attack that blacked out parts of Ukraine." *The Washington Post*, January 5. https://www.washingtonpost.com/world/national-security/russian-hackers-suspected-in-attack-that-blacked-out-parts-of-ukraine/2016/01/05/4056a4dc-b3de-11e5-a842-0feb51d1d124_story.html.

NATO CCD COE. 2017. "NotPetya and WannaCry Call for a Joint Response from International Community." https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/.

Navarrete, Iñaki, and Russell Buchan. 2019. "Out of the Legal Wilderness: Peacetime Espionage, International Law and the Existence of Customary Exceptions." *Cornell International Law Journal* 51 (4): 897–953. https://scholarship.law.cornell.edu/cilj/vol51/iss4/4.

Newsweek. 2016. "U.S. Says Cyber Attack Caused Ukraine Power Outage." *Newsweek,* February 25. https://www.newsweek.com/ukraine-power-outage-cyber-attack-russia-putin-sandworm-430556.

Ney, Paul C., Jr. 2020. "DOD General Counsel Remarks at U.S. Cyber Command Legal Conference." Speech by Hon. Paul C. Ney, Jr. on 2 March 2020. https://www.defense.gov/Newsroom/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/.

Nicolas, Ashley C. 2018. "Taming the Trolls: The Need for an International Legal Framework to Regulate State Use of Disinformation on Social Media." *The Georgetown Law Journal Online* 107: 36–62.

Nilsson, Hans G. 2006. "From Classical Judicial Cooperation to Mutual Recognition." *Revue Internationale de Droit Pénal* 77 (1-2): 53–58.

ODNI (Office of the Director of National Intelligence). 2017. Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution.

OEWG (Open-Ended Working Group). 2020b. Second "Pre-draft" of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security. https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf.

Ohlin, Jens David. 2018. "Election Interference: The Real Harm and The Only Solution." Cornell Legal Studies Research Paper No. 18: 18-50. https://ssrn.com/abstract=3276940.

Ohlin, Jens David. 2020. *Election Interference: International Law and the Future of Democracy*. Cambridge: Cambridge University Press.

OSCE. 2015. "Resolution on the Continuation of Clear, Gross and Uncorrected Violations of OSCE Commitments and International Norms by the Russian Federation." *Helsinki Final Declaration*. http://www.old.oscepa.org/meetings/annual-sessions/2015-helsinki-annual-session/2015-helsinki-final-declaration/2282-07.

Paganini, Pierluigi. 2020. "German investigators blame Russian DoppelPaymer gang for deadly hospital attack." *Security Affairs*, September 22. https://securityaffairs.co/wordpress/108620/malware/doppelpaymer-german-hospital-attack.html.

Park, Donghui, Julia Summers, and Michael Walstrom. 2017. "Cyberattack on Critical Infrastructure: Russia and the Ukrainian Power Grid Attacks". *University of Washington*, October 11. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/.

Peagler, Jordan. 2014. "The Stuxnet Attack: A New Form of Warfare and the (In)applicability of Current International Law." *Arizona Journal of International & Comparative Law* 31 (2): 399–434. http://arizonajournal.org/archive/vol-31-no-2/.

Pilloud, Claude, de Preux, Jean, Sandoz, Yves, Swinarski, Christophe, and Zimmerman, Bruno. 1987. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: International Committee of the Red Cross/Martinus Nijhoff Publishers.

Polityuk, Pavel. 2015. "Ukraine to probe suspected Russian cyber attack on grid." *Reuters*, December 31. https://www.reuters.com/article/us-ukraine-crisis-malware/ukraine-to-probe-suspected-russian-cyber-attack-on-grid-idUSKBN0UE0ZZ20151231.

Pompeo, Michael R. 2020. "The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector." U.S. Department of State, Press Statement, April 17. https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/.

Post, Kyiv. 2017. "Cyber attack fails to inflict major damage on Ukraine's security facilities." *Kyiv Post*, June 30. https://www.kyivpost.com/ukraine-politics/cyber-attack-fails-inflict-major-damage-ukraines-security-facilities.html.

"Power grid cyberattack in Ukraine (2015)". 2019. *International cyber law: interactive toolkit*. https://cyberlaw.ccdcoe.org/wiki/Power_grid_cyberattack_in_Ukraine_(2015).

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol). 2016. OJ L135/53, Article 3.

Richardson, John. 2011. "Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield." *The John Marshall Journal of Information Technology & Privacy Law* 29 (1): 1–28. https://repository.law.uic.edu/jitpl/vol29/iss1/1/.

Richmond, Jeremy. 2012. "Evolving Battlefields: Does Stuxnet Demonstrate a Need For Modifications to the Law of Armed Conflict?" *Fordham International Law Journal* 35 (3): 842–894. https://ir.lawnet.fordham.edu/ilj/vol35/iss3/1.

Rid, Thomas. 2018. "An Imperfect Weapon." *Survival* 60 (5): 227–232. doi:10.1080/00396338.2018.1518391.

Rid, Thomas, and Peter McBurney. 2012. "Cyber-Weapons." *The RUSI Journal* 157 (1): 6–13. doi:10.1080/03071847.2012.664354.

Rodríguez, Miguel. 2017. Declaration by Miguel Rodríguez, Representative of Cuba, at the Final Session of Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, June 23. https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf.

Roguski, Przemysław. 2020a. "Application of International Law to Cyber Operations: A Comparative Analysis of States' Views." The Hague Program for Cyber Norms Policy Brief, March. https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views.

Roguski, Przemysław. 2020b. "Russian Cyber Attacks Against Georgia, Public Attributions and Sovereignty in Cyberspace". *Just Security*, March 6. https://www.justsecurity.org/69019/russian-cyber-attacks-against-georgia-public-attributions-and-sovereignty-in-cyberspace/.

Roguski, Przemysław. 2020c. "The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States." *Just Security*, May 11. https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/.

Roguski, Przemysław. 2020d. "Iran Joins Discussions of Sovereignty and Non-Intervention in Cyberspace." *Just Security*, September 3. https://www.justsecurity.org/72181/iran-joins-discussions-of-sovereignty-and-non-intervention-in-cyberspace/.

Roscini, Marco. 2014. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

Rõigas, Henry. 2018. "Cyber War in Perspective: Lessons from the Conflict in Ukraine." In *A Civil-Military Response to Hybrid Threats*, edited by E. Cusumano, and M. Corbe, 233–257. London: Palgrave Macmillan.

Ruhl, Christian, Duncan Hollis, Wyatt Hoffman, and Tim Maurer. 2020. "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads." Carnegie Endowment for International Peace and Perry World House, Working Paper, February. https://carnegieendowment.org/2020/02/26/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-crossroads-pub-81110.

Sanger, David. 2012. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown Publishers.

Sanger, David. 2018. *The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age*. New York: Broadway Books.

Sassoli, Marco, Antoine Bouvier, Anne Quintin, and Julia Grignon. 2014. "Military Necessity". In *How Does Law Protect in War?* ICRC's Online Casebook. https://casebook.icrc.org/glossary/military-necessity.

Satariano, Adam, and Nicole Perlroth. 2019. "Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong." *The New York Times*, April 15. www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.

"Scenario 03: Cyber operation against the power grid.". 2020. *International cyber law: interactive toolkit*. https://cyberlaw.ccdcoe.org/wiki/Scenario_03:_Cyber_operation_against_the_power_grid#Prohibition_of_intervention.

"Scenario 14: Ransomware campaign.". 2020. *International cyber law: interactive toolkit*. https://cyberlaw.ccdcoe.org/wiki/Scenario_14:_Ransomware_campaign#cite_ref-55.

Schlesinger, Stephen. 1995. "Cryptanalysis For Peacetime: Codebreaking and the Birth and Structure of the United Nations." *Cryptologia* 19 (3): 217–235.

Schmitt, Michael N. 2012. "Attack as a Term of Art in International Law: The Cyber Operations Context." In *4th International Conference on Cyber Conflict*, edited by C. Czosseck, R. Ottis, and K. Ziolkowski, 283–293. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence.

Schmitt, Michael N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schmitt, Michael N., ed. 2017a. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Schmitt, Michael N. 2017b. "Grey Zones in the International Law of Cyberspace." *Yale Journal of International Law Online* 42 (2): 1–21.

Schmitt, Michael N. 2018. "Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." *Chicago Journal of International Law* 19 (1): 30–67. https://chicagounbound.uchicago.edu/cjil/vol19/iss1/2.

Schmitt, Michael N. 2020. "The Defense Department's Measured Take on International Law in Cyberspace." *Just Security*, March 11. https://www.justsecurity.org/69119/the-defense-departments-measured-take-on-international-law-in-cyberspace/.

Schmitt, Michael N., and Jeffrey Biller. 2017. "The NotPetya Cyber Operation as a Case Study of International Law." *EJIL: Talk!*, July 11. https://www.ejiltalk.org/the-notpetya-cyber-operation-as-a-case-study-of-international-law/.

Schmitt, Michael N., and Liis Vihul. 2017a. "Sovereignty in Cyberspace: *Lex Lata Vel Non?*" *AJIL Unbound* 111: 213–218.

Schmitt, Michael N., and Liis Vihul. 2017b. "Respect for Sovereignty in Cyberspace." *Texas Law Review* 95 (7): 1639–1671.

Segal, Adam. 2016. *Cyber Conflict After Stuxnet: Essays from the Other Bank of the Rubicon*. Vienna: Cyber Conflict Studies Association.

Sharp, Walter. G. 1999. *Cyberspace and the Use of Force*. Falls Church: Aegis Research Corporation.

Tsagourias, Nicholas. 2020. "Electoral Cyber Interference, Self-Determination, and the Principle of Non-Intervention in Cyberspace." In *Governing Cyberspace: Behavior, Power and Diplomacy*, edited by Dennis Broeders, and Bibi van den Berg, 45–63. London: Rowman & Littlefield International.

U.S. Department of the Treasury. 2018. "Treasury Sanctions Russian Cyber Actors for Interference with the 2016 U.S. Elections and Malicious Cyber-Attacks." March 15. https://home.treasury.gov/news/press-releases/sm0312.

UNGA (United Nations General Assembly). 2013. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc A/68/98, June 24. https://undocs.org/A/68/98.

UNGA (United Nations General Assembly). 2015. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. UN Doc A/70/174, July 22. https://undocs.org/A/70/174.

UNGA. 2018a. Resolution Adopted by the General Assembly on 5 December 2018 on Developments in the Field of Information and Telecommunications in the Context of International Security. A/RES/73/ 27.

UNGA. 2018b. Resolution Adopted by the General Assembly on 22 December 2018 on Advancing Responsible State behaviour in Cyberspace in the Context of International Security. A/RES/73/266.

UNGA (United Nations General Assembly). 2021a. Open-ended working group on developments in the field of information and telecommunications in the context of international security. Final Substantive Report. UN Doc A/AC.290/2021/CRP.2, March 10. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

UNGA (United Nations General Assembly). 2021b. Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. UN Doc A/76/135, July 14. https://www.undocs.org/pdf?symbol=en/A/76/135.

UNGA (United Nations General Assembly). 2021c. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266. UN Doc A/76/136, July 13. https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf.

UNGA (United Nations General Assembly). 2021d. Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security Third substantive session. Chair's Summary. UN Doc A/AC.290/2021/CRP.3, March 10. https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

United Kingdom's Foreign, Commonwealth & Development Office. 2018. "Foreign Office Minister condemns Russia for NotPetya attacks." Press release, February 15. https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

United Kingdom's Foreign, Commonwealth & Development Office. 2021. "Russia: UK and US expose global campaign of malign activity by Russian intelligence services". Press release, April 15. https://www.gov.uk/government/news/russia-uk-and-us-expose-global-campaigns-of-malign-activity-by-russian-intelligence-services.

Valuch, Jozef, and Ondrej Hamulak. 2018. "The right reference is Cyber Operations During the Conflict in Ukraine and the Role of International Law". In *The Use of Force Against Ukraine and International Law*, edited by S. Sayapin, and E. Tsybulenko, 215–235. The Hague: T.M.C. Asser Press.

Vanhecke, Nikolas, and Mark Eeckhaut. 2018. "Britten saboteerden onderzoek hacking Belgacom." *De Standaard*, October 25. https://www.standaard.be/cnt/dmf20181024_03869109.

Vervaele, John A. E. 2005. "Terrorism and Information Sharing Between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law?" *Utrecht Law Review* 1 (1): 1–27. http://doi.org/10.18352/ulr.1.

Volz, Dustin, and Jim Finkle. 2016. "U.S. helping Ukraine investigate power grid hack." *Reuters*, January 12. https://www.reuters.com/article/us-ukraine-cybersecurity-usa-idUSKCN0UQ24020160112.

Von Der Burchard, Hans. 2020. "Merkel blames Russia for 'outrageous' cyberattack on German parliament." *Politico*, May 13. https://www.politico.eu/article/merkel-blames-russia-for-outrageous-cyber-attack-on-german-parliament/.

Watson, F. Charlene. 2017. “Petya/NotPetya: Why it is Nastier Than WannaCry and Why We Should Care.” *ISACA Journal* 6: 1–6. https://www.isaca.org/resources/isaca-journal/issues/2017/volume-6/petyanotpetya-why-it-is-nastier-than-wannacry-and-why-we-should-care.

The White House. 2021. “Fact Sheet: Imposing Costs for Harmful Foreign Activities by the Russian Government.” April 15. https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/.

The White House. 2018. “Statement from the Press Secretary.” February 15. https://www.whitehouse.gov/briefings-statements/statement-press-secretary-25/.

Wrange, Pål. 2014. “Intervention in National and Private Cyberspace and International Law.” In *International Law and Changing Perceptions of Security: Liber Amicorum Said Mahmoudi*, edited by Jonas Ebbesson, Marie Jacobsson, Mark Klamberg, David Langlet, and Pål Wrange, 307–326. Leiden: Brill/Nijhoff.

Wright, Jeremy. 2018. “Cyber and International Law in the 21st Century”. Speech by Attorney General Jeremy Wright QC MP on 23 May 2018. https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World’s First Digital Weapon*. New York: Broadway Books.

Zetter, Kim. 2016a. “Inside the Cunning, Unprecedented Hack of Ukraine’s Power Grid.” *WIRED*, March 3. https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

Zetter, Kim. 2016b. “Everything We Know About Ukraine’s Power Plant Hack.” *WIRED*, January 20. https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/.