Journal of Cyber Policy

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

The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment

Dennis Broeders

To cite this article: Dennis Broeders (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, DOI: 10.1080/23738871.2021.1916976

To link to this article: https://doi.org/10.1080/23738871.2021.1916976

Published online: 26 Apr 2021.

JOURNAL OF CYBER POLICY
https://doi.org/10.1080/23738871.2021.1916976

Routledge
Taylor & Francis Group

The (im)possibilities of addressing election interference and the public core of the internet in the UN GGE and OEWG: a mid-process assessment

Dennis Broeders

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

ABSTRACT

This paper investigates whether and how the twin UN processes of the UN Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG) are willing and able to address two 'below-the-threshold' problems in their deliberations. The call for the protection of the public core of the internet and the call for the protection against foreign election interference have been flagged by many state and non-state parties for consideration by both processes. This paper analyses the threats that the vulnerability of the public core of the internet and foreign election interfere pose for stability in cyberspace, as well as the legal and normative proposals that have been suggested to promote responsible state behaviour. On the basis of the public documents that states have submitted to the more transparent OEWG process, the contours are sketched of what the inclusion of these issues in possible consensus reports for both processes may look like. The OEWG concluded its deliberations with a consensus report that addresses some aspects of these issues, shifting the task of further elaboration and guidance firstly onto the ongoing UN GGE process, as well as onto the new OEWG 2021–2025 and other UN processes that are emerging.

ARTICLE HISTORY
Received 4 November 2020
Revised 23 February 2021
Accepted 1 March 2021

KEYWORDS
Cyber security; cyber norms; diplomacy; UN GGE; OEWG

1. Introduction

The UN GGE produced consensus reports in 2010, 2013 and 2015, creating a rudimentary framework for thinking about conflict in cyberspace and possible ways to prevent and/or deal with such conflicts. The reports aim to provide legal and normative guidelines for responsible state behaviour in cyberspace and, given the fact that these reports were adopted by the UN General Assembly, they hold some normative sway. The core achievements of these reports may be summarised as follows. The 2010 report marks the first time that the experts were able to come to a consensus on the nature of the threat landscape in cyberspace (UN GGE 2010). The 2013 report states for the first time that the experts are of the opinion that international law applies in cyberspace as it does in the offline world. In other words, no special treaty for cyberspace is needed (UN GGE

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

2013). However, formulating this principle was also the start of a still ongoing debate on the question of what that means in practice: *how* does international law apply in cyberspace? The 2015 report reiterated and solidified the notion that international law applies in cyberspace and also introduced 11 non-binding and voluntary norms of responsible state behaviour (UN GGE 2015). The 2016–2017 round of the UN GGE did not produce a consensus report. The group was unable to reach consensus and, contrary to diplomatic traditions, the American expert and the Cuban expert both issued public statements on why the negotiations had failed in their view. The Cuban delegate accused the Western experts of trying to militarise cyberspace (Rodríguez 2017), while the American expert accused some experts in the GGE of backtracking on progress made in the earlier GGE reports (Markoff 2017). It seems that the bone of contention was the question of how international law – and especially International Humanitarian Law (IHL) – applies in cyberspace.

Currently, there are two UN processes dealing with the issue of responsible behaviour in cyberspace. Unable to reach consensus on a format for the renewed discussions, two resolutions were tabled and voted through by the UN General Assembly in late 2018: 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). As both resolutions were approved by the General Assembly, there are now two parallel processes in session that have a 90 per cent overlapping mandate, but a very different membership. The UN GGE (2019-2021) consists of 25 national experts who deliberate behind closed doors, while the OEWG (2019-2020) is open to all UN member states and deliberates in public. The current global COVID-19 pandemic has disturbed the proceedings of both processes, with both the OEWG and the UN GGE already behind their original schedule.

In the best-case scenario – with both groups producing consensus reports in 2021 – it will be six years after the last GGE consensus report of 2015. Cyber years are long. The period after the 2015 report includes cyber operations such as the attack on the Ukrainian power grid, the interference in the 2016 US presidential elections, the WannaCry attack and NotPetya to name a few of game-changing proportions. Since 2016, disinformation and foreign information operations (active measures) have become an integral part of the cyber security threat landscape (Rid 2020; Jankowicz 2020; Whyte 2020; Schia and Gjesvik 2020; Singer and Brooking 2018). All the high-profile cyber operations since 2015 fall below the threshold of an armed attack and do not trigger international humanitarian law. 'Below-the-threshold' operations create what Lucas Kello (2017) calls a situation of 'unpeace': not war in a legal sense but not friendly state relations either. Given that this is where the worries of many states are focussed, it would be a disappointing outcome if neither of the UN processes addressed any of them and thus failed to keep pace with how cyber conflict is developing.

Since 2015, debates about international law and norms in cyberspace have continued and picked up speed in the wake of the failure of the GGE to produce a consensus report in 2017. In the absence of a UN process, academia, regional organisations, national governments and multi-stakeholder settings continued the work on norms and international law (see, for example, Hurel and Cruz Labato 2018; Ott and Osula 2019; Roguski 2020; Eggenschwiler and Kulesza 2020). This paper looks at the developments around two issues that have emerged in these debates about responsible behaviour in cyberspace.

Firstly, the debate about the protection of the public core of the internet has been ongoing since 2015 (Broeders 2015; 2017) and has picked up support at the multi-stakeholder level (GCSC 2017b, 2019; the *Paris Call for Trust and Security in Cyberspace*) and gained the support of governments (for example Government of the Netherlands 2017) and the EU (EU 2019; EC 2020). It has met with approval and with resistance, but has persistently been a part of the cyber norms debate since 2015. Moreover, an attack on, or interference with, the public core of the internet – the internet's core protocols and infrastructure – would be a 'high impact, low probability' issue that is generally considered to be of interest to the UN GGE. Secondly, the issue of election interference has been put firmly on the agenda since the well-documented case of the 2016 US presidential elections (Ohlin 2020; Egloff 2020; Buchanan 2020; ODNI 2017). Embedded in the larger global debate about disinformation and information operations, election interference is an issue that has surfaced in an increasing number of countries (Schia and Gjesvik 2020; Hollis and Neutze 2021). Given the fact that elections determine the distribution of political power and – in democratic states – are an expression of the political will of the people, many states are trying to find a way to address the issue internationally, including in the GGE and OEWG processes.

This paper will investigate both the possibilities and the (likely) impediments for the GGE and the OEWG to address and take a position on these issues. At the time of finalising this paper, the OEWG had just concluded its work with a consensus report, while the UN GGE was still ongoing. Both the concluded and the continuing diplomatic negotiations on these issues take place against a general background of rising geopolitical tensions not least of all between the USA, China and Russia, which are key players inside and outside cyberspace. Section 2 will outline the problems and the threats associated with the public core of the internet and with election interference. Section 3 will discuss proposals and possible solutions to these problems that have been suggested by various actors from academia, civil society and government. Section 4 looks at how the OEWG has, and how the UN GGE might, address these issues, on the basis of the scarce, but publicly available, state contributions to the proceedings of the OEWG. The analysis focuses both on process and (possible) outcome. Statements of support or resistance are found in these state submissions to the OEWG and also in official government statements on the interpretation of international law in cyberspace. Section 5 draws some modest conclusions, as these processes are not in the hands of academics, but in those of states playing multilevel games.

2. Two 'new' problems

Neither the vulnerability of the public core of the internet, nor election interference, are new problems. They are only new in the sense that they have recently been specifically articulated and surfaced in the debate about responsible state behaviour in cyberspace, which means that they have been flagged as a risk and/or as a problem. Since 2015 both these issues have been debated in several fora and have gained traction with an increasing number of state and non-state actors. As such they have also become part of the current negotiations of the UN OEWG and UN GGE. Whether they will be part of the final consensus reports – if the groups are able to reach consensus – and in what form, is a separate matter.

The vulnerability of the public core of the internet

The public core of the internet is comprised of the main protocols and infrastructure of the global internet, which can be considered a global public good. This global public good does not comprise the whole of the internet or even enter into the content layer of the internet but is limited to the logical and physical infrastructural layers of the core internet (Broeders 2015). It can be considered a global public good as the functionality and the integrity of the public core of the internet benefits a large global public and the benefits are quasi-universal (Kaul et al. 1999). There are two basic approaches to determining what is covered by the concept the public core (Broeders 2017: 368-369). The first approach to defining the public core is *layered* and distinguishes three basic layers – logical, physical and organisational. The logical layer includes central protocols like TCP/IP, DNS and routing protocols; the physical layer includes core infrastructure like DNS servers and sea cables; and the organisational layer includes internet exchanges and CERTs. The concept is not set in stone. So while it is clear that key parts of the logical and physical infrastructure are part of the core of the internet – such as TCP/IP, DNS and routing, and DNS servers and internet exchanges – it is less evident where inclusion would stop. The second approach to defining the public core is *functional*. Instead of listing what should or should not belong to the public core of the internet, it emphasises what the public core of the internet *does*. The public core is then defined as the general availability and integrity of the core forwarding and naming functions of the global internet (Broeders 2017: 369; GCSC 2017a and 2019).[1]

The problem with the core logical and technical infrastructure of the internet is that it has not been designed from a perspective of security. Or, as one of the founding fathers of the internet, David Clark, once said: 'It's not that we didn't think about security … We knew that there were untrustworthy people out there, and we thought we could exclude them' (cited in Timberg 2015).

There are basically two threats to the public core of the internet. The first threat results from interference with the workings of the core protocols in such a way that it would lead to a splintering of the internet at the deep level of the naming and forwarding functions of the internet. Interference with the root zone or data localisation that require changes in routing protocols (Drake, Cerf and Kleinwächter 2016) – may damage the functioning of the public core. Technical translations of digital sovereignty, like the Russian plans for a RuNet which would only route traffic inside Russia's borders, would damage global internet traffic if they were successfully implemented. However, the technical challenges are such that the Russian plan is for now more a geopolitical gesture than a technical reality (Kurowska 2020).

Another threat to the public core is its vulnerability to attack or misuse. An early reminder of the vulnerability of the BGP and DNS system was Pakistan's blocking of YouTube in 2008, which had worldwide repercussions.[2] This early example shows just how tightly interwoven the internet is through its core protocols, and how vulnerable those protocols are to national actions (DeNardis 2014: 96). A blunt approach to taking down the world wide web is through public core protocols such as DNS (Schneier 2016). The DDoS attack on Dyn in 2016, an American DNS provider, is a case in point. The Mirai botnet – famous for being largely composed of IoT devices – knocked Dyn offline, creating severe disruption to internet traffic in the United States, and even affecting parts of

Europe. Should this have happened in a smaller country the effects of such an attack would have been profoundly transnational. The Border Gateway Protocol (BGP), a core routing protocol, could also be vulnerable to attack. BGP hijacks and leaks have been a common problem for a long time, even though in recent years the technical community has been working to decrease the problem of BGP leaks, for example by cryptographically validating secure routes (Newman 2020). As there is no hierarchy between the BGP speaking routers, updates by a single BGP speaker can impact routing information in the entire internet. Not all, or even most, hijacks are intentional, showing the relative ease with which the main protocols can be used to misdirect traffic. Rerouting of traffic through the ISPs of a specific country can be used for mass surveillance and intelligence-gathering and potentially for sabotage. In a more general sense, they undermine trust in the integrity and trustworthiness of the internet.

The potential to do real damage with a determined attack via BGP and/or DNS is much greater than we have seen so far. Experts estimate that ultimately the value of these vulnerabilities is much bigger for sabotage than for intelligence-gathering. The fact that we have not seen attacks like this at their full potential is not necessarily reassuring. 'What if' scenarios for high impact, low probability events seldom are. It is also not a reason to not worry about them from a national and international security perspective. The NSA wrote a memo in 1985 about the dangers of 'viral infection' and 'denial of service', well before the Morris worm proved that this was more than a theoretical possibility (Corera 2015: 141).

Election interference

States have always tried to interfere in each other's political processes through the use of information and disinformation. Thomas Rid's book *Active Measures* (2020) gives a history of disinformation campaigns from the early twentieth century until the current, digital era. According to Rid (2020: 14), disinformation became more dangerous in the digital era: 'The internet did not bring more precision to the art and science of disinformation – it made active measures less measured: harder to control, harder to steer, and harder to isolate engineered effects.' For many, the story of disinformation and election interference broke in 2016/2017 when the details of Russian interference in the US presidential election started coming out. By now, digital interference in other countries' internal affairs is becoming more commonplace and disinformation seems to become a part of the foreign operations playbook of an increasing number of states (Whyte 2020; Bradshaw and Howard 2019). Against a general background of rising disinformation campaigns, election interference stands out as a specific concern for especially, but not solely, liberal democratic states. Civil society organisations and governments from democratic states have been championing the cause to get protection of the electoral process into the proceedings of the OEWG and the UN GGE.

The problem of election interference is Janus-faced: it amounts to a violation of the holy grail of democracy – free and fair elections – but the interference itself hardly involves any serious crime (Broeders 2020). The Russian interference in the 2016 US presidential election may serve as a case in point. The events are well documented in official US documents (ODNI 2017; Muller 2019) and in academic accounts (Egloff 2020; Rid 2020; Buchanon 2020; Kilovaty 2018; Ohlin 2020). This operation – attributed to the Russian

military intelligence agency GRU and believed to be ordered by President Putin himself – was composed of three cyber operations. The first two were 'hack and leak' operations. Russian hackers broke into the accounts of the Democratic National Congress and into the email account of John Podesta, who was at that time serving as Hillary Clinton's campaign manager, and stole a large amount of confidential emails and documents. These were later leaked to the general public and the media through various outlets, including WikiLeaks, at politically significant times such as 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. They were clearly intended to damage the Clinton campaign and influence the American presidential elections. The third operation was the online 'trolling campaign' on social media aimed at influencing the thinking of American voters. Russian actors impersonating American citizens and organisations were using social media platforms to sow division and heighten nativist tendencies. Especially the *covert* impersonation of American citizens is flagged by some scholars as legally significant (Ohlin 2020, Tsougarias 2020; Schmitt 2018).

Hack and leak operations – often hack, *forge* and leak operations that mix real and doctored information – involve computer crime that violates criminal law. The online trolling, or what Singer and Brooking (2018) call the 'weaponization of social media', is to a large extent legal, but does involve some crime of identity theft and impersonation. But overall, there is an imbalance in the larger crime committed – interfering with the democratic process – and the charges that criminal law allows. To many observers, crime and punishment do not seem balanced. Moreover, under domestic criminal law only individuals (the actual perpetrators, GRU officers) can be charged. Legally, the finger cannot be pointed at the state behind the operation (although putting pictures of hackers in Russian military uniforms on FBI posters serves that function informally).

3. Arguing the case for protection: norms advocacy

Both the protection of the public core of the internet and the protection of election processes have been debated, adopted and propagated by various stakeholders. Norms processes require champions, time and ultimately (near) consensus to solidify the acceptance of, and adherence to, a norm. That goes both for norms in international politics in general (Finnemore and Sikkink 1998) and for cyber norms processes (Finnemore and Hollis 2016; Maurer 2019). What should be taken into account is that cyber norms processes will be (even) more contested in years to come than they have been since the 2017 GGE failed to produce a consensus report (Maurer 2019; Kurowska 2019). Rising geopolitical tensions, an increase in cyber-aware and cyber-active states and the OEWG process that includes all states, make normative diversity and adversity between normative positions a feature of both UN processes. The public core of the internet is usually debated under the umbrella of cyber norms, whereas the protection of election processes is debated both in terms of cyber norms and in terms of international law. Although in the context of the UN GGE it should be emphasised that norms and international law can and do mutually reinforce each other and should not be seen as two completely different and parallel discourses (Adamson 2020). In recent years, a number of state and multi-stakeholder initiatives have been paving the way for these two issues.

Calls to protect the public core of the internet

The call to protect the public core of the internet was originally formulated as a standard of restraint among states: 'In order to protect the Internet as a global public good there is a need to establish and disseminate an international standard stipulating that the Internet's public core – its main protocols and infrastructure, which are a global public good – must be safeguarded against intervention by governments' (Broeders 2015: 95). As such it is a proscriptive norm that tells the group that adheres to it what they should not do (Finnemore and Hollis 2016: 444). In 2017, the Netherlands made the protection of the public core of the internet part of its International Cyber Strategy, underscoring that the public core 'possesses elements of an international public good that transcends individual sovereign and private interests' and that 'given our dependence on the internet, it is necessary to exercise restraint when engaging in activities that can affect that public core' (Government of the Netherlands 2017: 5). In 2017, the multistakeholder Global Commission on the Stability of Cyberspace (GCSC) addressed the public core in the first of a series of norm proposals. Taking a functional approach to the protection of the public core, widening it to non-state actors and linking it to the overall stability of cyberspace, the commission stipulated that 'Without prejudice to their rights and obligations, state and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace' (GCSC 2017a, 2019: 21). By directing the norm explicitly at activity that 'intentionally and substantially' damages the public core, the commission addressed the fact that many states will allow their militaries and intelligence agencies to conduct operations 'using' the internet's key protocols and infrastructure, even when they would not allow and approve of inflicting substantial damage with transnational effects to it. Also, this formulation is in itself already a nod to the norm that states should not attack each other's critical infrastructure stated by the 2015 UN GGE consensus report. In November 2018, on the commemoration of the Armistice, the French government launched the *Paris Call for Trust and Security in Cyberspace* (2018), which includes a number of norms proposals. The document, which is open to signatures from all stakeholders in cyberspace, stipulates that the signatories will work together to 'prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet'. The Paris call is not a legally binding document but has been signed by 78 states – including all EU member states – and nearly a thousand civil society organisations and companies.[3] Lastly, in 2019 the EU included the responsibility to protect the public core of the internet in the EU Cyber Security Act and stated that 'ENISA should support the security of the public core of the open internet and the stability of its functioning, including, but not limited to, key protocols (in particular DNS, BGP, and IPv6), the operation of the domain name system (such as the operation of all top-level domains), and the operation of the root zone' (EU 2019: 151/19, see also 151/35).

These calls for a normative protection of the public core of the internet are mostly formulated as a call for restraint on behalf of states, and sometimes also non-state actors and/or state proxies, in their dealings with the core internet. However, states do not lightly enter into self-restraint as they may view it as being at odds with their national (security) interests. States may gain a strategic advantage if they keep the possibility of conducting attacks on or through the public core on the table, or reversely, suffer a

potential disadvantage if they pledge to refrain from doing so. Given that states cannot be certain that other states will uphold a non-binding norm, some object to the call for protection of the public core on grounds of national security considerations. While this argument cannot be fully discarded there are also potential severe national security considerations that result from a lack of protection of the public core (Broeders 2017: 372-373). Similarly, some states resist the idea that the core of the internet is a global public good, insisting instead that the internet is ultimately physical and therefore part of the territorial sovereignty of states. Although some parts of the core internet are indeed physically part of the world of states (cables, internet exchanges), the logical infrastructure is not territorial in any real sense. Moreover, the internal logic of how the internet functions technically makes it very easy to create transnational or downstream effects when interfering with the public core, even when the infrastructure resides on sovereign soil (Broeders 2017: 370-372; Mueller 2019).

Calls to protect election processes

Protection against election interference has some strong defenders and has spurned debates on the role of international law as well as on the role of non-binding norms to address the issue (Hollis and Neutze 2021.

The Global Commission on the Stability of Cyberspace proposed a norm for the protection of election infrastructure in 2018: '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.' Again, a proscriptive norm of self-restraint. Later in 2018, the *Paris Call for Trust and Security in Cyberspace* also addressed the issue of election interference, calling on its signatories to cooperate to 'strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities'. Whereas the GCSC specifically addresses the technical election infrastructure, the Paris norm focuses on 'election processes', which could be interpreted as broader than just the technological infrastructure. On the other hand, the Paris norm is focused on capacity-building and prevention but does not, unlike the GCSC, explicitly condemn election interference other than calling the activities 'malign' and 'malicious'. States have also flagged their concern. For example, the G7 (2017) issued a *Declaration on Responsible State Behavior in Cyberspace*, expressing their concern 'about cyber-enabled interference in democratic political processes'. In 2018, they doubled down in the *Charlevoix Commitment on Defending Democracy from Foreign Threats*, pledging to 'strengthen G7 cooperation to prevent, thwart and respond to malign interference by foreign actors aimed at undermining the democratic processes and the national interests of a G7 state' (G7 2017). The G7 statements seem to address the broader problem of foreign undermining of democratic processes, and focus on cooperation, prevention and response. In terms of the rule or norm that the G7 sees as being violated, they mention sovereignty and in a very general sense 'the rules-based international order' and 'international norms'.

In parallel to these norm proposals, states and legal scholars have been discussing whether and how election interference amounts to a violation of international law. As countries are starting to set out their views on how international law applies to state conduct in cyberspace, some have flagged election interference as a possible breach of

international law, or more specifically as a breach of the non-intervention rule (Roguski 2020: 29-31; Moynihan 2020: 11). The Netherlands (2020a) 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.' 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 (2016), 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.' Australia (2020), 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.' These statements all point to 'manipulation' and 'altering the results' as a threshold value. This is however hard to measure, let alone prove, in such a multi-causal process as elections.[4]

Many legal scholars see non-intervention as the way forward, even though some issues need to be addressed to make the problem of election interference in cyberspace fit the requirements (see for example Schmitt 2018; Hollis and Neutze 2021; Roguski 2020). Making election interference fit with the conditions to qualify as illegal intervention, i.e. (a) being coercive and (b) interfering in the *domaine réservé* of a state, will require in the words of Kilovaty (2018: 152), 'a new layer of legal subtlety'. Tsagourias (2020) adds such a layer by connecting the violation of the principle of non-intervention 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; 2020) goes a step further and 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.

4. Fitting norms into the UN processes

Advocating norms – especially when they are aimed at state behaviour – will ultimately have to land in agreements that are negotiated between states in order to gain a stronger foothold.[5] In the case of cyber norms and interpretations of international law in relation to cyberspace, the UN GGE has traditionally been the forum where these discussions take place at the global level. Since 2019, the UN GGE shares that limelight with the parallel process of the OEWG. How these parallel processes will influence each other – especially in light of the geopolitical tensions from which they were born – is hard to say at the time of writing. In diplomacy the true lie of the land is often revealed only in the endgame.

The new OEWG process has one specific advantage, especially for the research community. Where the UN GGE deliberates behind closed doors and only reveals its end product – if it achieves consensus on a report – the OEWG deliberates in public. Moreover, states have been submitting written contributions to the deliberations publicly as well. The

OEWG website[6] contains many written state contributions to the proceedings and some states even submit the same input papers to both processes. As the OEWG is formally a multilateral process – as opposed to the UN GGE where, strictly speaking, it is not states but experts making the contributions[7] – these contributions reflect official state positions. Although no diplomatic process unfolds itself fully in daylight, the OEWG contributions provide insights into the UN diplomatic process on international cybersecurity that have been lacking with closed UN GGE negotiations. However, since the outbreak of the COVID-19 pandemic, the deliberations of the OEWG have moved online but have also gone darker with respect to the general public as the informal sessions are not public, meaning that transparency of the process has decreased.

In case of the OEWG we know the chapter headings, and their order, of the final report (see Table 1). The adoption by consensus of the Final Substantive Report on 12 March 2021 held a few surprises in both structure and content. The discussion sections that were part of both the zero draft and the first draft of the substantive report – on which consensus seemed unlikely – were cut out of the Final Substantive report and moved to a Chair's summary on which no consensus is needed (Chair OEWG 2021a, 2021b, 2021c, 2021d). Moreover, the order of the chapters on international law and norms was reversed in the final report: the chapter on norms now comes before the chapter on international law, which was an explicit wish of China. Most of the like-minded countries opposed this switch, but did not want to sacrifice consensus on this issue. The UN GGE reports from 2010, 2013 and 2015 all have different structures in terms of chapter headings, adding topics over the years. However, the mandate of the current UN GGE as formulated in the resolution overlaps by and large with the headings used in the OEWG pre-draft reports, as well as with the general structure of the 2015 UN GGE report. The main differences are the annex for the UN GGE report and the section on 'regular institutional dialogue' for the OEWG report. Table 1 gives a good indication of the blueprint(s) into which the issues of the protection of the public core of the internet and the protection of election processes would have to be inserted.

There are minimal and maximal outcomes possible. The most negative scenario – neither process ends in the publication of a report – has been averted with the adoption of a final report of the OEWG. It is also possible that only the OEWG results in a report, but that is less likely as the UN GGE and the OEWG seem locked in a situation of Mutually

Table 1. The expected structure of the UN GGE and OEWG reports.

UN GGE[1]	OEWG[2]
(A) Introduction	A. Introduction
(B) Possible cooperative measures to address *existing and potential threats* in the sphere of information security	B. Conclusions and recommendations Existing and potential threats
(C) How *international law* applies to the use of information and communications technologies by states	Rules, norms and principles for responsible state behaviour International law
(D) Norms, rules and principles of responsible behaviour of states	Confidence-building measures Capacity-building
(E) Confidence-building measures	Regular institutional dialogue
(F) Capacity-building	C. Final observations
(G) Conclusions and recommendations	ANNEX: Chair's summary
(H) ANNEX containing national contributions of participating governmental experts on the subject of how international law applies	

[1]The sections (B)-(F) and (H) are based on the mandate of the UN GGE as written down in paragraph 3, page 3 of the resolution
[2]OEWG Chair 2021c.
Source: OEWG Chair (2021c), UNGA 2018b, art 3, page 3.

Assured Diplomacy and are more likely to either fail or succeed together (Broeders 2019). The risk that some states might sabotage the UN GGE because the OEWG has already secured a report, while a distinct possibility, is mitigated by the fact that Russia has already put a new resolution on the table – and got it approved by the UN General Assembly (UN GA 2021) – to set up a new round of the OEWG 2021-2025. Sabotaging the UNGGE would be likely to have negative repercussions for this next OEWG that Russia, as instigator and champion of the OEWG process, would like to avoid. The most positive scenario is that both issues get taken up in the report(s) in all the relevant chapters. Considering the 'blueprint' and chapter headings of table 1 that would mean (1) being flagged as a threat, (2) introduced as a new norm and/or specified as a violation of international law and (3) being supported by cooperative measures in the sections on cooperative measures, CBMs and/or capacity-building. To a certain extent, 'new norms' face an uphill struggle in the UN processes as some states have signalled that they do not wish to add new norms, but want to focus on implementation and on providing an additional layer of understanding of the current set of norms from the 2015 GGE report. Forging consensus on the OEWG report was partially done by slowly pushing out all the text that was non-consensual and indicating that 'some states' were in favour of a certain notion. In the zero draft, this text was placed in 'discussion' sections of each chapter (Chair OEWG 2021a). In the first draft of the substantive report all the discussion sections were taken out of the various chapters and grouped together in a new, second part of the report under the general heading 'discussions' (Chair OEWG 2021b). The fact that this text was in italics already suggested that it would not make it into the final report. In the Final Substantive Report the discussion section was taken out of the consensus report entirely and placed in the annexed Chair's Summary (Chair OEWG 2021c, 2021d), leaving a short consensus report.

The public core of the internet

The Netherlands (2020b) flagged the vulnerability of the public core in its first contribution to the OEWG and GGE for inclusion in both the threat chapter and in the norms chapter. The Dutch propose to connect the protection of the public core of the internet to the 2015 GGE norm on the protection of critical infrastructures (13(f)), as an additional layer of the current norm. As a specification it is argued that (some) critical infrastructure is no longer solely confined to the borders of states but is increasingly becoming transnational and interdependent. The public core of the internet, as an example of such a transnational critical infrastructure, should be protected using language tailored to that of the 2015 report:

> State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace as guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g) (The Netherlands 2020b)

The first pre-draft of the OEWG report picked up on the issue of the public core of the internet. It included the issue in the norms chapter of the report, indicating 'that the general availability or integrity of the public core of the Internet should be protected' (Chair OEWG 2020a, section 38). In the same chapter, the report also says that: 'States

also highlighted that supranational critical information infrastructure could be considered a special category of critical infrastructure, and that its protection was the shared responsibility of all States.' In the conclusion the chair connects the issue to capacity-building: 'Member States [are] encouraged to further cooperate to build capacity to identify and protect national and transnational critical infrastructure as well as supranational critical information infrastructure' (page 15).

With a first draft on the table, states were getting more specific in their comments. Both the notion of transnational critical infrastructure and the public core of the internet received support, questions and opposition. The debate about transnational infrastructure got muddied because there are a number of different concepts circulating in various state contributions that point to the same phenomenon but are not exactly the same. The US (2020) picked up on the fact that OEWG delegates were talking about 'supranational', 'trans-border' and 'transnational' critical infrastructure, but it was not clear to the US delegation if 'delegates were using those terms interchangeably or not'. The US was 'also unsure what it means to declare 'supranational critical information infrastructure' a 'special category' of such infrastructure, with protection that is a 'shared responsibility' of all States', thus diplomatically taking position against the supranational idea, but leaving room to find consensus on one of the other concepts. Japan (2020) and Estonia (2020) also took issue with the lack of clarity on the issue. Estonia furthermore highlights that most critical information infrastructure 'resides within national a jurisdictions, while Japan expresses concern that these 'unclear concepts … may lead to the undervaluation of the importance of national critical infrastructure.' This echoes the territorial sovereignty objection discussed in section three of this paper. Other countries, such as Singapore (2020), Switzerland (2020), the Netherlands (2020c) and Germany (2020), highlight it as a 'useful addition to the already existing norms on the protection of critical infrastructure', explicitly supporting the notion of transnational critical infrastructure. The EU (2020) is also supportive: 'critical infrastructures are no longer confined to the borders of States but are increasingly becoming transnational and interdependent.'

The concept of the public core itself received support and questions as well. There is substantial support to flag the concept in the threat section and in the norms section (see Brazil 2020; EU 2020; Switzerland 2020; the Netherlands 2020c; Germany 2020). Germany (2020) sees the norm for the protection of the public core of the internet as a useful addition for 'enhancing existing norms and improving their understanding and implementation' and explicitly flags it as guidance for the implementation of UN GGE 2015 recommendation 13(f) and 13(g) (see also the Netherlands 2020c). China (2020) however has indicated that 'given the limited amount of time we have, attention should also be drawn to avoid introducing concepts that have not gained global consensus yet ('public core' for instance) into the report.' The UK (2020) indicated early that it has a problem with the letter – but not with the spirit – of the public core concept: 'We also remain concerned about the concept of internet having a public core, while fully supporting idea that general availability of internet must be protected.'

The revised pre-draft of the OEWG maintains the (unchanged) reference to the protection of the public core in its norms chapter (OEWG Chair 2020b: section 42). The revised report has also started to address the conceptual confusion around transnational critical infrastructures – while keeping the issue on board. In the threat chapter the report

highlights that 'CI and CII may be shared or networked with another State or operated across different States and jurisdictions (sometimes categorised as transborder, transnational or supranational infrastructure)', adding that these infrastructures are in need of 'inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability' (section 23). It revisits the issue in the norms chapter of the pre-draft: 'States also highlighted that the protection of transborder critical information infrastructure, as a distinct category of critical infrastructure, is the shared responsibility of all States' (section 42). A general call for cooperation to protect transnational infrastructure is also part of the conclusions of the report with respect to capacity-building.

The zero, first and final draft of the OEWG report all retain the notion of transnational infrastructure in the threats section. The final report states that critical infrastructure 'may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability' (Chair OEWG 2021c, section 18). The protection of the public core has made it into the zero draft but no longer under that name. In the discussion section – indicating no full consensus – of the norms chapter it states that proposals were made that 'drew attention to the importance of cooperating to protect critical infrastructure that crosses borders or jurisdictions, as well as the importance of ensuring the general availability and integrity of the Internet' (section 50). In the first draft of the final report a similar formulation was moved to the consensus part of the document and in the final draft a reference was included in both the threats and the norms section of the report. The final report flags malicious ICT activities 'that impact the general availability or integrity of the Internet' as 'a real and growing concern' in the threat section and underscores the need for states to 'endeavor to ensure the availability and integrity of the Internet' in the norms section (Chair OEWG 2021c).

Election interference

The first round of contributions to the OEWG saw a number of states flagging election interference as a threat, with some countries emphasising the problem of disinformation 'to undermine trust and confidence in political and democratic processes and institutions' (Switzerland 2020) or more broadly 'targeted efforts to undermine political systems and elections' (New Zealand 2020). The Netherlands (2020b) flagged 'the threat of malign interference by foreign actors aimed at undermining electoral processes' as 'real and credible'. Moreover, China (2020) under the heading of state sovereignty, suggests a form of a norm: 'States should refrain from using ICTs to interfere in internal affairs of other states and undermine their political, economic and social stability.' The Netherlands (2020b) also proposes addressing the issue under the norms chapter, aligning itself with the norm proposal of the Global Commission on the Stability of Cyberspace, and again tailoring the language to the infrastructure norms of the 2015 GGE report:

> The Netherlands would like to suggest therefore that the OEWG and GGE consider the recommendation that 'State and non-state actors must not pursue, support or allow cyberoperations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites,' as guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g).

Australia's (2019) contribution breaks open the case of addressing election interference under the international law section, arguing 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, intervention in the fundamental operation of Parliament, or in the stability of States' financial systems would constitute a violation of the principle of nonintervention.'

The first pre-draft of the report mentions the threat of 'information operations and disinformation campaigns' in a general sense, without mentioning election interference specifically (Chair OEWG 2020a, section 15). In section 19, it is noted that states 'emphasized the severity of threats to particular categories of infrastructure, including for instance the health and financial sectors and electoral infrastructure', indicating that the Chair is channelling the discussion towards electoral infrastructure rather than the broader notion of electoral processes. In the chapter on norms, the pre-draft indicates that 'States should not conduct ICT operations intended to disrupt the infrastructure essential to political processes' (section 38), which is broad-ranging but still connected to the word infrastructure.

The first draft report solicited new views on the issue of election interference in the state submissions following its publication. General support for flagging the issue under the threats chapter ranged from minimal to extremely broad-ranging. France (2020) simply indicates that 'more space could be dedicated to field of vital importance such as healthcare, finance, transport, and electoral infrastructures [*sic*]', while Zimbabwe (2020) drew in the role and responsibilities of (social) media platforms:

> We reiterate concern over the prevalent misuse of media platforms, including social media networks, for hostile propaganda, interference in the internal affairs of other States, dissemination of discriminatory and distorted information of events such as election results, and campaigns that defame and incite hatred among citizens.

Ecuador (2020) and Brazil (2020) also underscore the threat to election infrastructures, linking the issue to national critical infrastructure protection and in the case of Ecuador echoing the language used by the GCSC and the Netherlands. A number of states are now advocating to protect election infrastructure. Brazil (2020) states that 'the IT infrastructures underpinning electoral processes also deserve the same protection accorded to the public core of the Internet'. Pakistan (2020), Ecuador (2020), the Netherlands (2020c) and Germany (2020) all propose a norm that should protect the 'technical infrastructure essential to political processes, such as elections, referenda or plebiscites'. Germany and the Netherlands again present this norm as a guidance for implementation of UN GGE 2015 norms on critical infrastructure protection. There are no specific comments to support or oppose Australia's suggestion to mark election interference as a violation of the principle of non-intervention under the international law chapter of the report. However, as indicated above, there is an increasing number of states that have published their vision on the applicability of international law in cyberspace with some of them naming election interference as a possible violation of the principle of non-intervention. Given that the UN GGE report is envisioned to have an annex comprised of state positions on international law, there is a possibility that this issue might land in/be annexed to a GGE report, if consensus can be reached.

All drafts up to the final report mention electoral processes in the threats section, but the accompanying norm got deleted in the zero draft and did not return. The later drafts,

including the final report, use a revised formulation in the threats section that links the issue more directly to the underlying (critical) infrastructure: 'Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern' (Chair OEWG 2021c, section 18).

The limits of the paper trail

While the relative transparency of the OEWG gives analysts much more information than has ever been available during previous rounds of the UN GGE process, we should also be careful to avoid looking for our lost keys under the streetlight just because that is where the light shines. While the OEWG cracks open the black box of diplomacy, we do not and cannot know how much of the deliberations we get to see – diplomacy has traditionally and legitimately been afforded a certain right to secrecy – nor which information we can take at face value and which information is strategic or even misleading. Moreover, it stands to reason that states with more resources and a diplomatic track record on these issues are more likely to put their contributions on paper, while less experienced states may make up their minds as the process unfolds without submitting a written contribution. Some states will also refrain from submitting a written contribution as a negotiation strategy, not wishing to bind their hands and allowing themselves more room to manoeuvre. As a result, support for some proposals may be much broader or much more limited than it seems on the basis of the paper trail. The formal and informal negotiations will determine the outcome.

5. Discussion

A mid-process assessment of a diplomatic negotiation is a risky endeavour at the best of times. An assessment of two parallel diplomatic negotiations, one finished and one ongoing, against a background of rising geopolitical tensions both inside the subject domain (cyberspace) and outside it, paves the way for a modest discussion and conclusion. In diplomacy, nothing is agreed until all is agreed. With that in mind this paper has documented the emergence of two issues – the call to protect the public core of the internet and the call to protect against election interference – in the international debate about responsible state behaviour in cyberspace. Both issues have acquired advocates among state and non-state actors and the thinking on the nature and size of the problem and possible normative ways to address those have been gaining support. For both issues the push and initial support has come predominantly – but certainly not exclusively – from liberal democratic states, but they are now being debated in the global fora of the UN GGE and the OEWG. Given the current state of the debate at the UN – especially since the adoption of the OEWG consensus report – it is clear that there is a viable path to address both these issues. The OEWG final report addressed the issue of the protection of the public core of the internet – albeit in modified language – in both the threat section and the norms section, and flagged the vulnerability of the infrastructure underlying political and electoral processes as a threat. The fact that this now represents the consensus of all UN member states will have an impact on the ongoing UN GGE process. The darkest scenario is that OEWG consensus will be used to

sabotage the current UN GGE by reasoning that the international community now has a better, inclusive, all-member state process that can generate consensus on the matter of international security in cyberspace. If that scenario does not play out, the OEWG report may work as an accelerator for these two issues. Given that all the states that are involved in the UN GGE are also part of the consensus on the OEWG, it would be impossible to deny that these are now issues of importance to the international community. Moreover, if we take the 2015 UN GGE report as a benchmark then a new GGE report would be expected to be more detailed and precise in character than the OEWG final report, thus raising the stakes for the UN GGE to come up with more precise wording and guidance on the issues at hand in cyberspace, including the protection of the public core of the internet and election interference.

Already the debate is moving towards what will happen *after* both of the current processes conclude, with France and Egypt, and a broad coalition, pushing for a Programme of Action (see Géry and Delerue 2020) and Russia already having secured a new OEWG for the years 2021-2025. Both the new OEWG and the PoA are likely to continue to work on a number of issues that were discussed in recent years, not least of all because many of those proposals ended up in the Chair's summary (Chair OEWG 2021d), which according to section 80 of the OEWG consensus report 'should be further considered in future UN processes, including in the Open-Ended Working Group established pursuant to General Assembly resolution 75/240' (Chair OEWG 2021c). No matter how the UN deliberations on responsible behaviour in cyberspace will unfold exactly, it is likely that we will continue to live in 'interesting cyber times' for the foreseeable future.

Notes

1. The GCSC in 2018 also published a short technical note on what the commission considers needs to be included in the public core of the internet (GCSC 2018).
2. In 2008, the Pakistani Ministry of Information ordered YouTube to be blocked in Pakistan but the change it made to the routing protocol not only affected Pakistani ISPs, but was broadcast and adopted globally, causing YouTube to become inaccessible across the entire internet.
3. At the time of writing, the current list and number of signatories can be found here: https://www.diplomatie.gouv.fr/en/french-foreign-policy/united-nations/multilateralism-a-principle-of-action-for-france/alliance-for-multilateralism-63158/article/paris-call-for-trust-and-security-in-cyberspace
4. See, for example, Benkler, Faris and Roberts (2018) for a critical view on the importance of foreign election interference.
5. Although in the end, it is state behaviour that determines whether something is truly a norm among states.
6. https://www.un.org/disarmament/open-ended-working-group/
7. Even though that is officially how the GGE is represented, the experts are invariably state diplomats/government officials working on matters of international cybersecurity. The UN GGE is a diplomatic, multilateral process in nature, even if it is not in name.

Disclosure statement

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

Funding

This work was supported by the Ministerie van Buitenlandse Zaken.

Notes on contributor

Dennis Broeders is Professor of Global Security and Technology and Senior Fellow of The Hague Program for Cyber Norms at the Institute of Security and Global Affairs of Leiden University, the Netherlands. His research and teaching broadly focuses on the interaction between security, technology and policy, with a specific interest in international cyber security governance and diplomacy. He is the author of the book *The public Core of the Internet* (2015) and co-editor of the book *Governing Cyberspace: Behavior, Power and Diplomacy* (2020).

References

Adamson, L. 2020. "International Law and International Cyber Norms: A Continuum?" In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders, and B. van den Berg. London: Rowman & Littlefield.

Benkler, Y., R. Faris, and H. Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford: Oxford University Press.

Bradshaw, S., and P. Howard. 2019. *The Global Disinformation Order. 2019 Global Inventory of Organised Social Media Manipulation*. Oxford: Oxford Internet Institute.

Broeders, D. 2015. *The Public Core of the Internet. An International Agenda for Internet Governance*. Amsterdam: Amsterdam University Press.

Broeders, D. 2017. "Aligning the International Protection of 'The Public Core of the Internet' with State Sovereignty and National Security." *Journal of Cyber Policy* 2 (3): 366–376.

Broeders, D. 2019. "Mutually Assured Diplomacy: Governance, 'Unpeace' and Diplomacy in Cyberspace." *Global Policy – Digital Debates* 6: 26–29.

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

Buchanan, B. 2020. *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics*. Cambridge, MA: Harvard University Press.

Corera, G. 2015. *Intercept. The Secret History of Computers and Spies*. London: Weidenfeld and Nicolson.

DeNardis, L. 2014. *The Global War for Internet Governance*. New Haven: Yale University Press.

Drake, W., V. Cerf, and W. Kleinwächter. 2016. *Internet Fragmentation: An Overview. Future of the Internet Initiative White Paper*, January 2016. World Economic Forum. http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

EC. 2020. The EU's Cybersecurity Strategy for the Digital Decade. Joint Communication to the European Parliament and the Council by the High Representative of the Union for Foreign Affairs and Security Policy. Brussels, 16 Dec. JOIN (2020) 18 final.

Egan, B. 2016. *Remarks on International Law and Stability in Cyberspace*. Remarks by Brian J. Egan, Legal Adviser to the US Department of State. 10 November.

Eggenschwiler, J., and J. Kulesza. 2020. ""Non-State Actors as Shapers of Customary Standards of Responsible Behaviour in Cyberspace."." In *Governing Cyberspace: Behaviour, Power and Diplomacy*, edited by D. Broeders, and B. van den Berg. London: Rowman & Littlefield.

Egloff, F. 2020. "Contested Public Attributions of Cyber Incidents and the Role of Academia." *Contemporary Security Policy* 41 (1): 55–81.

EU. 2019. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

Finnemore, M., and D. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110 (3): 425–479.
Finnemore, M., and K. Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52 (4): 887–917.
G7. 2017. Declaration on Responsible States Behavior in Cyberspace (Lucca, 11 April). https://www.mofa.go.jp/files/000246367.pdf.
GCSC. 2017a. *Call to Protect the Public Core of the Internet*. New Delhi, November. https://cyberstability.org/wp-content/uploads/2018/07/call-to-protect-the-public-core-of-the-internet.pdf.
GCSC. 2017b. *Definition of the Public Core, to Which the Norm Applies*. Bratislava, May. https://cyberstability.org/wp-content/uploads/2018/07/Definition-of-the-Public-Core-of-the-Internet.pdf.
GCSC. 2018. *Call to Protect the Electoral Infrastructure*. Bratislava, May. https://cyberstability.org/wp-content/uploads/2018/05/GCSC-Call-to-Protect-Electoral-Infrastructure.pdf.
GCSC. 2019. *Advancing Cyberstability. Final Report of the Global Commission on the Stability of Cyberspace*. November.
Géry, A., and F. Delerue. 2020. "A New UN Path to Cyber Stability." (6 October) *Directions. Cyber Digital Europe*. https://directionsblog.eu/a-new-un-path-to-cyber-stability/.
Government of the Netherlands. 2017. "Building Digital Bridges." International Cyber Strategy: towards an integrated international cyber policy. https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy.
Hollis, D., and J. Neutze. 2021. ""Defending Democracies via Cybernorms."." In *Defending Democracies: Combatting Foreign Election Interference in a Digital Age*, edited by D. B. Hollis, and J. D. Ohlin. Oxford: Oxford University Press.
Hurel, L. M., and L. Cruz Lobato. 2018. "Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs." *Journal of Cyber Policy* 3 (1): 61–76.
Jankowicz, N. 2020. *How to Lose the Information War. Russia, Fake News and the Future of Conflict*. London: I.B. Taurus and Company.
Kaul, I., I. Grunberg, and M. Stern. 1999. "Defining Global Public Goods." In *Global Public Goods. International Cooperation in the 21st Century*, edited by I. Kaul, I. Grunberg, and M. Stern, 2–19. New York: UNDP.
Kello, L. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.
Kilovaty, I. 2018. "Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information." *Harvard National Security Journal* 146.
Kurowska, X. 2019. "The Politics of Cyber Norms: Beyond Norm Construction towards Strategic Narrative Contestation." *EU Cyber Direct: Research in Focus*.
Kurowska, X. 2020. "On the Geopolitics of Russia's Sovereign Internet Law." *ISPI Dossier*, 2 April. https://www.ispionline.it/en/pubblicazione/geopolitics-russias-sovereign-internet-law-25428.
Markoff, M. 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." 23 June. 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.
Maurer, T. 2019. "A Dose of Realism: The Contestation and Politics of Cyber Norms." *Hague Journal on the Rule of Law* 12: 283–305.
Moynihan, H. 2020. "The Vital Role of International law in the Framework for Responsible State Behaviour in Cyberspace." *Journal of Cyber Policy*, online first, 1–16.
Mueller, M. 2019. "Against Sovereignty in Cyberspace." *International Studies Review*, 1–23.
Mueller, R. S., III. 2019. *Report on the Investigation into Russian Interference in the 2016 Presidential Election* (2 vols). https://www.justice.gov/storage/report.pdf.
Newman, L. H. 2020. "A Broken Piece of Internet Backbone Might Finally Get Fixed." *Wired*, 12.02.2020. https://www.wired.com/story/bgp-routing-manrs-google-fix/.

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

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

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

Ott, N., A. Osula, et al. 2019. "The Rise of the Regionals: How Regional Organisations Contribute to International Cyber Stability Negotiations at the United Nations Level." In *11th International Conference on Cyber Conflict: Silent Battle*, edited by T. Minarik, 321–346. Tallinn: CCDCOE.

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

Rid, Th. 2020. *Active Measures. The Secret History of Disinformation and Political Warfare*. New York: Farrar, Strauss and Giroux.

Rodríguez, M. 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. 23 June. https://www.justsecurity.org/wp-content/uploads/2017/06/Cuban-Expert-Declaration.pdf.

Roguski, P. 2020. *Application of International Law to Cyber Operations: A Comparative Analysis of States' Views*. The Hague Program for Cyber Norms Policy Brief. March.

Schia, N. N., and L. Gjesvik. 2020. "Hacking Democracy: Managing Influence Campaigns and Disinformation in the Digital age." *Journal of Cyber Policy*, online first, 1–16.

Schmitt, M. 2018. "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law." *Chicago Journal of International Law* 19 (1): 30–67.

Schneier, B. 2016. "Someone Is Learning How to Take Down the Internet." *Lawfare*, 13 September. https://www.lawfareblog.com/someone-learning-how-take-down-internet.

Singer, P. W., and E. T. Brooking. 2018. *LikeWar. The Weaponization of Social Media*. New York: Houghton Mifflin Harcourt Publising.

Timberg, G. 2015. "A flaw in the design. The Internet's founders saw its promise but didn't foresee users attacking one another." *Washington Post*, 25 May.

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

UN GA. 2021. *Resolution Adopted by the General Assembly on 31 December* 2020 *on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*. A/Res/75/240, 4 January.

UN GGE. 2010. *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*. UNGA. A/65/201 New York: UN.

UN GGE. 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, 24 June. https://undocs.org/A/68/98.

UNGGE. 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, 22 July. 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.

Whyte, C. 2020. "Cyber Conflict or Democracy 'Hacked'? How Cyber Operations Enhance Information Warfare." *Journal of Cybersecurity* 6 (1): 1–17.

Wright, J. 2018. *Cyber and International Law in the 21st Century*. Speech by Attorney General Jeremy Wright QC MP at Chatham House London on 23 May.

OEWG documents

Australia. 2019. Australian paper – Open Ended Working Group on developments in the field of information and telecommunications in the context of international security, September 2020. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf.

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

Brazil. 2020. Comments submitted by Brazil to the Initial '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/2020/04/comments-by-brazil-on-the-pre-draft-report-of-cyber-oewg-8-apr-2020.pdf.

Chair of the OEWG. 2020a. Initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 27 April. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/200311-Pre-Draft-OEWG-ICT.pdf.

Chair of the OEWG. 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. 27 May. https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf.

Chair of the OEWG. 2021a. Draft Substantive Report (Zero Draft) of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 19 January. https://undocs.org/A/AC.290/2021/L.2.

Chair of the OEWG. 2021b. Substantive Report (First Draft) of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 1 March. https://front.un-arm.org/wp-content/uploads/2021/03/210301-First-Draft.pdf.

Chair of the OEWG. 2021c. Final Substantive Report of the report of the OEWG on developments in the field of information and telecommunications in the context of international security. 10 March. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

Chair of the OEWG. 2021d. Chair's Summary of the OEWG on developments in the field of information and telecommunications in the context of international security. 10 March. https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

China. 2020. China's Contribution to the Initial Pre-Draft of OEWG Report. https://front.un-arm.org/wp-content/uploads/2020/04/china-contribution-to-oewg-pre-draft-report-final.pdf.

EU. 2020. Joint comments from the EU and its Member States on the initial 'pre-draft' report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security. https://front.un-arm.org/wp-content/uploads/2020/05/eu-contribution-alignments-oewg.pdf.

Ecuador. 2020. Ecuador preliminary comments to the Chair's 'Initial pre-draft' of the Report of the United Nations Open Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG). https://front.un-arm.org/wp-content/uploads/2020/04/ecuador-comments-on-initial-pre-draft-oewg.pdf.

Estonia. 2020. Estonia's comments to the 'Initial "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/2020/04/comments-to-the-oewg-pre-draft-report-estonia.pdf.

France. 2020. France's response to the pre-draft report from the OEWG Chair. https://front.un-arm.org/wp-content/uploads/2020/04/contribution-fr-oewg-eng-vf.pdf.

Germany. 2020. Initial 'Pre-draft' of the report of the OEWG on developments in the field of information and telecommunications in the context of international security and non-paper listing specific language proposals under agenda item 'Rules, norms and principles' from written submissions received before 2 March 2020. Comments from Germany. https://front.un-arm.org/wp-

content/uploads/2020/04/20200401-oewg-german-written-contribution-to-pre-draft-report-1.pdf.

Japan. 2020. Japan's Position Paper on the Initial 'Pre-draft' of the Report of the United Nations Open-Ended Working Group on 'Developments in the Field of Information and Telecommunications in the Context of International Security'. https://front.un-arm.org/wp-content/uploads/2020/04/japan-comments-on-oewg-pre-draft.pdf.

New Zealand. 2020. Position Paper on New Zealand's Participation in the February 2020 Session of the 2019-2020 Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/nz-position-paper-on-oewg.pdf.

Singapore. 2020. Singapore's written comment on the chair's pre-draft of the OEWG report. https://front.un-arm.org/wp-content/uploads/2020/04/singapore-written-comment-on-pre-draft-oewg-report.pdf.

Switzerland. 2020. UN Open-ended working group on developments in the field of information and telecommunications in the context of international security, 2019/2020 Written feedback by Switzerland to the first pre-draft report of the OEWG. https://front.un-arm.org/wp-content/uploads/2020/04/20200409-switzerland-remarks-oewg-pre-draft.pdf.

The Netherlands. 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.

The Netherlands. 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.

The Netherlands. 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.

Pakistan. 2020. Pakistan's inputs in response to the letter dated 11 March 2020 from the Chair of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG). https://front.un-arm.org/wp-content/uploads/2020/05/inputs-on-pre-draft-of-oewg-report-revised.pdf.

The UK. 2020. Contribution by United Kingdom to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the context of International Security, February. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/03/20200303-uk-national-contribution-oewg2.pdf.

The US. 2020. United States Comments on the Chair's Pre-draft of the Report of the UN Open Ended Working Group (OEWG). https://front.un-arm.org/wp-content/uploads/2020/04/oewg-pre-draft-usg-comments-4-6-2020.pdf.

Zimbabwe. 2020. Considerations on the initial pre-draft of the open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security. https://front.un-arm.org/wp-content/uploads/2020/04/zimbabwe-position-on-pre-draft-of-oweg-final-report.pdf.