



# The unexpected norm-setters: Intelligence agencies in cyberspace

Ilina Georgieva

To cite this article: Ilina Georgieva (2020) The unexpected norm-setters: Intelligence agencies in cyberspace, Contemporary Security Policy, 41:1, 33-54, DOI: [10.1080/13523260.2019.1677389](https://doi.org/10.1080/13523260.2019.1677389)

To link to this article: <https://doi.org/10.1080/13523260.2019.1677389>



© 2019 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 09 Oct 2019.



Submit your article to this journal [↗](#)



Article views: 2547



View related articles [↗](#)



View Crossmark data [↗](#)



Citing articles: 1 View citing articles [↗](#)

# The unexpected norm-setters: Intelligence agencies in cyberspace

Ilina Georgieva 

Institute of Security and Global Affairs, Faculty of Governance and Global Affairs, Leiden University, The Netherlands



## ABSTRACT

By implementing novel intelligence techniques in cyberspace, security and intelligence agencies have become major actors in the cybersecurity landscape. As they no longer just passively gather information for their governments but conduct both defense and offense operations in cyberspace, they signal international actors that their conduct is at least tolerable, even if not officially acceptable. Thereby, the intelligence agencies generate norms for the rest of the international community. Yet, they remain under the international regulation radar for being sub-state entities. Consequently, the main argument of this article is the following: To prevent the hollowing-out of cyber regulation efforts, the norm-setting role of intelligence actors should be taken into account when designing cyber norms.

**KEYWORDS** Global cyber norms; intelligence agencies; norm-setters; norm development; cybersecurity policy; regulation

International cybersecurity regulation is still in its infancy due to ongoing debates on how international law applies to the cyber domain. Cyber norms processes—designed to create some general rules of the road in the mean-time—have also not come to fruition yet. This is partially due to the inherently slow nature of creating international regulations, where agreements even among friends are laborious. A further reason is the general preference of international actors for strategic ambiguity (Broeders, Boeke, & Georgieva, 2019, p. 3) when dealing with quickly evolving cyber threats and capabilities. Not committing to a regulatory framework helps them buy time, while exploring and stretching both technological and normative boundaries.

This article adds a further reason to this list. It argues that regulation strategies to date have not factored in all major actors whose conduct in cyberspace

**CONTACT** Ilina Georgieva  [i.n.georgieva@fgga.leidenuniv.nl](mailto:i.n.georgieva@fgga.leidenuniv.nl)  Institute of Security and Global Affairs, Faculty of Governance and Global Affairs, Leiden University, The Netherlands

© 2019 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial-NoDerivatives License (<http://creativecommons.org/licenses/by-nc-nd/4.0/>), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited, and is not altered, transformed, or built upon in any way.

matters. The use and development of cyber capabilities by security and intelligence agencies have turned them into major international actors. By implementing novel intelligence techniques in cyberspace, they signal international actors of all shapes and sizes that their conduct is tolerable, even if not officially acceptable. The agencies thereby generate norms for the rest of the international community. Yet, they remain under the international regulation radar for being sub-state entities. Consequently, the main argument of this article is the following: To prevent the hollowing-out of cyber regulation efforts, the norm-setting role of intelligence actors should be taken into account when designing cyber norms in the first place.

It is necessary to consider intelligence practices within ongoing cyberspace regulation debates due to major internal and external transformations in intelligence workings. Internally, technological advancement coupled with the pervasiveness of information and communication technologies (ICT) have blurred the contours of traditional intelligence activities. Fears of “going dark” in the advent of the information age have transformed intelligence actors from passive gatherers to hunters in cyberspace (Loleski, 2019, p. 120). Their “hunting” role has made them responsible for some of the most notorious cyber operations to date (Boeke & Broeders, 2018, p. 77, 85). This has played a crucial role in putting in motion processes of cyber regulation. Externally, events such as the Snowden disclosures and the Shadow Brokers leaks, which publicized intelligence techniques, have lured intelligence agencies out of the traditional shadows in two unprecedented ways. First, by triggering legislation reforms across jurisdictions, while, second, simultaneously forcing agencies to be vocal and thus visible as never before.

This article examines a particular technique of infiltrating computer networks to gather intelligence data (i.e., computer network exploitation or CNE), in order to exemplify the norm-setting impact of intelligence agencies. The exploitation technique portrays a norm of cyber espionage that is widely implemented by the intelligence community. This is in stark contrast with the official narratives of “responsible behavior in cyberspace” the governments of the same agencies preach. Admittedly, in the intelligence and national security context, divergence between actual intelligence practices and official governmental positions is not unusual. However, evidencing a norm on cyber espionage moves beyond the realm of foreign offices, since the latter only deal with intelligence crises and narratives once those reach the public. Such norm has far-reaching effects for the much disputed relationship between cyber espionage and international law in general, and the debate on cyber norms in particular. The espionage norm pinpoints a crucial moment in the formation of international norms—the instance in which the communal conduct spills over and is out in the open stimulating a discussion on the meaning of the practice

for the international community. In the intelligence context this means that intelligence practices seize to be secret.

Consequently, the value of the intelligence norm in question goes beyond policy chatter. It is widely recognized that secret practice is irrelevant for the development of legal rules (Bethlehem, 2012, p. 35, 36; Buchan, 2018, p. 152; Committee on the Formation of Customary (General) International Law, 2000, p. 15; Shaw, 2014, p. 53 referring to “overt actions”). In order for a particular norm to be recognized and even crystallize as customary international law, it must undergo “an iterative process of claim and response” (Perina, 2015, p. 567). This means an elaborate “contrast and compare” exercise with other relevant obligations of the involved actors. In norms literature, such a process is referred to as the practice of norm contestation, which not only puts the norm’s social meaning to the test (Engelkamp & Glaab, 2015, p. 203), but also introduces opportunities for norm transformation in external communities (Krook & True, 2012, p. 122).

Thus, this article puts forth that the norm’s visibility, combined with the norm-setting capacity of intelligence agencies, questions not only fundamental international codification processes, but also their aptitude for dealing with contemporary normative challenges inherent in the cyber domain. This warrants attention to bottom-up rule-making by intelligence actors, as otherwise, the dichotomy between international law-making and the practice-led norms by intelligence agencies is only going to widen.

To evidence the cyber espionage norm, this article looks into the National Security Agency’s (NSA) network infiltration technique Territorial Dispute (TeDi) (Greenberg, 2018a; Zetter, 2018), which was found in the 2017 Shadow Brokers leak. TeDi’s case portrays a clear-cut example of cyber espionage. The latter is a targeted cyber operation, which aims at infiltrating a particular system/network in order to obtain precise bits of otherwise unattainable information. Therein lies the precise value of examining an operation such as TeDi: It allows to make a clear distinction from a non-targeted intelligence operation, which brings about different legal and normative implications (i.e., bulk data collection or programs such as BULLRUN that tamper with communications encryption in various ways, and consequently affect Internet infrastructure on a global scale (Ball, Borger, & Greenwald, 2013)).

This article substantiates TeDi’s normative implications through insights from international relations norms literature and contemporary research on networked governance. The latter emphasizes the level of sub-state actors (Kooiman, 1999; Rhodes, 2007), such as the intelligence agencies, and their role in a myriad of governance structures, including those pertaining to cyberspace. The conceptions of networked governance notionally break up the “unitary” actor assumption and identify the relevant agents that adhere to, interpret, and seek to shape norms (Erskine & Carr, 2016, p. 97, 98). International relations literature in turn provides the conceptual tools to

“dissect” a norm into its building blocks—behavior, identity, propriety, and expectations (Finnemore & Hollis, 2016, pp. 438–444).

These blocks allow to trace the process and different stages of norm development. Such bottom-up approach is essential in the case at hand, since studying the normative implications of an intelligence tool implies evaluating its usage and thus the behavior it enables. Further, a bottom-up perspective toward norms is preferable, since both critics and advocates of the cyber norms processes have primarily concerned themselves with the (desired) content of norms, that is to say with what norms say or ought to say, not the process of creation of norms. While content analysis has certainly its merits, it alone is incomplete (Hollis, 2017, p. 3), as norms are inherently social, interaction-based (Finnemore & Sikkink, 1998), and often have effects beyond those originally envisioned (Finnemore & Hollis, 2019, p. 22, 23). By positioning the TeDi espionage norm within ongoing cyber norms debates, this article factors in the building blocks of a norm, the effects of interaction processes within particular groups and contexts, and what strategic choices those mirror. These have, thus far, been largely overlooked in the official cyber norms processes.

This article proceeds as follows. By going over the technical features that are most relevant to make the case of the cyber espionage norm, the next section presents TeDi and its forensic analysis. The following section then sets the scene for the normative discussion by briefly sketching the origin and most important developments in the cyber norms debates to date. The latter shows that current debates on cyber regulation leave little room for actors other than states. The article then zooms into the changed intelligence workings and the agencies’ strained relationship with international law. Here, the current article suggests networked governance as a lens through which the intelligence agencies’ practices and their impact on cyber regulation can be understood. The last section then elaborates on the cyber espionage norm portrayed by the use of TeDi by drawing on constructivist norms literature.

## **The Shadow Brokers and Territorial Dispute**

Between the summer of 2016 and the spring of 2017, an unidentified hacking group calling itself “The Shadow Brokers” published on the Internet stolen information about NSA exploitation tools in five subsequent leaks (Biddle, 2016; Nakashima & Timberg, 2017; Sanger, 2016). A particular piece of software found in the fifth (and so far final) leak caught the attention of technical security researchers based at the Laboratory of Cryptography and System Security (CrySyS) at the Budapest University of Technology and Economics. The team of scientists studied the software for about a year before publishing an extensive report on its features (Bencsáth, 2018) and ascertaining that the

examined code pertained to the cyber tool kit of the NSA's special operations team Territorial Dispute (TeDi) (Greenberg, 2018a; Zetter, 2018).

The agency had reportedly assembled TeDi after Chinese hackers stole designs for the military's joint strike fighter plane together with other sensitive data from U.S. defense contractors in 2007 (Zetter, 2018). Though originally intended as a unit to detect and counter online attackers in real time, TeDi's mission eventually evolved into providing situational awareness. The NSA unit did so by means of scripts and scanning tools to detect the presence of external parties, state-sponsored parties as it turned out, on machines it infiltrated (Zetter, 2018). Put simply, TeDi was spying on other spies.

The software scans for 45 different types of malware (numbered SIG1 to SIG45) (Bencsáth, 2018, p. 14, 15) by searching for particular files or registry keys (indicators of compromise or IoCs) the programs leave on compromised computers. However, while security researchers often amass dozens or even hundreds of IoCs to identify a hacking group (Zetter, 2018), TeDi needed only a few high quality signatures to correctly place a malware's origin (Bencsáth, 2018, p. 4). Moreover, the researchers discovered that the software contained detailed instructions for the NSA operators running it. Upon detecting specific code, operators should either try to learn more about the attack vectors, that is to say about the infected computer, its security software and the malware found on it; seek the advice of a supervisor; or immediately pull back (Bencsáth, 2018, p. 4). The instructions show the NSA's intention to study the exploitation tools of other foreign intelligence actors, while simultaneously avoiding tensions with other parties and minimizing the risk of detection and compromise of its own operations (Zetter, 2018).

The CrySys team managed to identify 23 of the 45 malware entries (Greenberg, 2018a) by matching elements of TeDi with known malware samples from their own research database. They discovered that in 2013—the year the tools are believed to have been stolen by the Shadow Brokers—the NSA was aware of and tracking some now well-known state-sponsored operations long before those unraveled and became public (Bencsáth, 2018, p. 5, 6). The malware samples CrySys could not place are suspected to be still ongoing operations (Zetter, 2018).

SIG1 and SIG2, for instance, match the code of Russian state hackers (Bencsáth, 2018, p. 16), one of which infected the Pentagon's networks back in 2008. Matches were also established between SIG entries and the Chinese hacking tool used in the 2010 Google hack (Zetter, 2010) and the North Korean hack "Dark Hotel" (Greenberg, 2018a; Zetter, 2014). Further, the team found that SIG8 matched the code of Stuxnet, the joint NSA-Israeli creation that managed to set back Iran's nuclear ambitions. While it is not unusual for intelligence agencies to scan for the code of close allies to stay out of each other's way, Stuxnet's presence on the list appears to have been part of a "cleanup effort" (Zetter, 2018). SIG 8 had been added to the

TeDi list in 2010 after Stuxnet had started to spread uncontrollably—spreading that eventually led to its detection and public exposure (Zetter, 2018).

Overall, the forensic analysis brings forward valuable insights into how much the NSA knows about advanced persistent threats (APTs) from external governmental attack operators, and how this knowledge is handled in practice. The article comes back to the software and operational particularities of TeDi and their implications for the emergence of particular cyber norms below.

### **Everyday norms: The why and how of cyber norms**

TeDi's bearing pertains to the broader debate on the centrality of cyberspace to contemporary (state) security matters (Stevens, 2012, p. 148) and our dependency on ICTs in nearly all sectors of modern society. The current state of affairs is exemplified by a number of incidents ranging from cyber-attacks towards private entities such as Sony Pictures (Peterson, 2014) to APTs like BlackEnergy targeting critical infrastructure (Kaspersky Lab, 2019) or the malware NotPetya intended to cause indiscriminate damage across the board (Greenberg, 2018b). While strategic assessment of such events is increasingly accompanied by regulation efforts that aim to make conduct in cyberspace more predictable and thus more secure for all parties involved, it took more than a decade to actually get the debate going and another ten to switch to the next gear. The following section succinctly traces the roots of cyber regulation efforts up until today in order to show how and why the international community started deliberating on cyber norms. The historical flashback is necessary in order to grasp the regulatory approaches and their underlying rationales, and to point to some of their inherent shortcomings in conceptualizing cyber norms.

Cybersecurity regulation started gaining momentum shortly after the politically-motivated cyber-attacks experienced by Estonia in 2007 and Georgia in 2008 (Stevens, 2012, p. 148). Ever since then, the major powers of the international community have been engaging in efforts to pin down the “dos and don'ts” of ICT use and promote responsible behavior in cyberspace by means of broadly shared norms, or cyber norms (see, for instance, Langevin, Mccaul, Charney, & Lewis, 2008). The latter would lay down informal or quasi-formal standards of conduct deemed a desirable alternative to a formal treaty. The norms approach granted its advocates maneuvering space that would not be available under “hard legalization” practices (Abbott & Snidal, 2000), allowing them to explore the impact of the initiated agreement while simultaneously looking into the exploitation of further technological developments. After all, verifying an adversary's treaty compliance would not only be difficult (Farrell & Glaser, 2017, p. 14), but would also mean a limitation of one's own (offensive) cyber capabilities (Farrell & Glaser, 2017, p. 14).

The idea of cyber norms first gained traction among the United States, the United Kingdom, and their allies. Anticipating conflicts of interest and ideologies, both United States' and United Kingdom's efforts from that time—the U.S. International Strategy for Cyberspace (Executive Office of the President of the United States, 2011) and the bringing into life of what became known as The London Process (Foreign & Commonwealth Office and The Rt Hon William Hague, 2011)—aimed at starting a dialogue among like-minded countries to lay down the foundation of the desired normative approach. Their rhetoric and advocacy efforts eventually swayed the process of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) process as well. The latter, although off to a slow start with its first mandate in 2004/2005 (Henriksen, 2019, p. 2), concluded its second convening period in 2009/2010 with a report recommending among other the further exploration of norms as a means of regulation by states (United Nations, 2010). Accordingly, the third (2012/2013) and fourth (2014/2015) UN GGE continued to explore potential cyber norms solutions to existing threats and risks to international peace and security in cyberspace. The UN GGE and the cyber norms approach—though birthed under the auspices of different sponsors and strategic considerations—had ended up (at least for a while) merged together, resulting in the UN GGE becoming the venue for addressing the future of cyber norms.

### **Regulation by whom and for whom?**

The UN GGE has, however, been anything but a smooth ride. Some questioned early on what an agreement on global cyber norms would look like, what the sources of such norms would be, and which actors should be involved in the norm-developing process (Hurwitz, 2014, p. 323). The lack of involvement of the industry, which owns nearly the entire physical infrastructure of the Internet and thereby holds a unique first responder position, for instance, was seen as a pitfall of the state-dominant UN GGE process (Hurwitz, 2014, p. 325). The norm development process itself was also seen as fraught: Advocated sets of norms appeared to be “hammered out” (Stevens, 2012, p. 165) through diplomacy and other forms of negotiation without paying due regard to the existing contexts in which norms were sought (Finnemore & Hollis, 2016, p. 427). Consequently, proposed cyber norms were designed to restate desired consequences and not to regulate actual conduct. As such, the UN GGE process omitted to factor in that norms are social constructs, and that behavioral patterns emerge through coping with the continued development of the respective normative context.

The fact that the UN GGE in 2017/2018 could not reach a consensus and therefore produced no concluding report reinforced doubts about the viability



of cyber norms (Grigsby, 2017; Henriksen, 2019; Tikk & Kerttunen, 2017). Practitioners and scholars alike have proclaimed the end of the UN GGE process. Some have argued that given the diverging power dynamics, strategic and ideological context, consensus on anything but the most basic of issues should not be expected at (Henriksen, 2019, p. 2, 4). After all, Russia and China—though participating in the forums of the UN GGE—had worked all along together with fellow members of the Shanghai Cooperation Organization on developing and promoting their own information security norms (United Nations, 2011; United Nations, 2015). That in combination with strongly colliding positions on the free flow of information, the applicability of International Humanitarian Law and the doctrine of state responsibility in cyberspace (Tikk-Ringas, 2017, p. 52) had driven the final wedge between the Sino-Russian coalition and its Western counterpart.

For the sake of good order, it should be noted that multiple non-state stakeholders actively partake in the global norms debate. The two most prominent examples from the private sector are Microsoft (Smith, 2017; McKay, Neutze, Nicholas, & Sullivan, 2014; Microsoft, 2016) and Siemens (Siemens et al., 2018), which joined the call for cyber norms with proposals for specific behavior standards (Macák, 2017, p. 888) directed primarily at the conduct of states. Other non-state actors such as (academic) think tanks like The Hague Program for Cyber Norms (HPCN, 2018), and joint initiatives as the Estonia-based NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE, 2017), and the Global Commission on the Stability of Cyberspace (GCSC, 2016) are also active in the norms debate. The former looks into existing international law and translates it to the cyber domain by means of the Tallinn Manual process. The latter's mandate is to develop proposals for norms and policies to enhance international security and stability, and to promote awareness on responsible behavior in cyberspace among different communities working on cybersecurity-related issues.

Additions to the stakeholder group partaking in the cyber norms debate do alleviate some of the criticism toward who should be included in the norm-making process. These, however, leave the reproach of the end goal (the norms for whom part) and of the norm-generating process, for the most part, unaffected. The reason for that can be found in the underlying regulatory approach. The latter is informed by a rational that has naturally governed international relations up until now—rules pronounced for states by states/state-sponsored mechanisms—that consequently targets states and their behavior as exclusive, unitary entities. While, undoubtedly, only states can create legally binding instruments under international law, their conduct is not the only cause of concern that effectively shapes the debate on norms in cyberspace (Farrell, 2015, p. 2). It might even not be the most important one.

Even if less visible to the public eye, non-state and sub-state actors build, run, and manage the everyday architecture of cyberspace (Farrell, 2015;

Hansen & Nissenbaum, 2009, p. 1161, 1162), and implicitly influence the arguments about the domain's regulation. By means of their practices, they play important roles in indicating regulation gaps that should be filled in the law-making process (Henriksen, 2019, p. 7). Those are not only private sector entities located, for instance, in the Silicon Valley. Sub-state entities like intelligence and security agencies autonomously develop and implement their own technological tools that fit their desired ends. The latter—although undoubtedly part of the state apparatus and largely covered by national regulatory frameworks—are steered by mandates and operational rational quite different from that of other public bodies. What is more, they are not easily comprehensible by outsiders (Stout & Warner, 2018; see also Ziolkowski, 2013, p. 427) by virtue of their inherent organizational secrecy.

It should also come as no surprise that most of the cyber incidents/attacks that put the cyber norms wheel in motion in the first place are the suspected and often skillfully attributed (see for instance, Council on Foreign Relations, 2019) work of intelligence agencies (Boeke & Broeders, 2018, p. 74). One need only think of Stuxnet, Belgacom, or WannaCry, to name just a few. Norms in the global cyber regulation debate, as technology itself, serve calculated aspirations (Tikk-Ringas, 2017, p. 47). Yet, when the norms omit to factor in the origin of the technology and the actual trouble-makers behind it, the regulation debate is to some extent “set in the wrong key” (Boeke & Broeders, 2018, p. 74). To remedy this state of affairs, the further conceptualization of the global cyber norms agenda should partially break with conventional regulation patters and dig deeper—at the sub-state level where the (questionable) behavioral standard is created and replicated by others. In that regard it is still a classic case of norm construction—one simply needs to focus on the right norm-propelling entity and take it from there.

### **Intelligence agencies as norm-setters**

Comprehending the capabilities and intentions of others has always been an inherent part of statecraft (Chesterman, 2006, p. 1072) and an essential part of a state's toolbox when handling foreign affairs (Lubin, 2016, p. 23). Consequently, intelligence activities—that is the collection, processing and analyzing of raw intelligence—have been long recognized as inherent features of the modern state's organizational apparatus (Demarest, 1995, p. 321). So how does one exactly make the notional jump from regarding the intelligence agencies as mere state attributes to conceptualizing them as norm-setters? By following the thickening red thread of their activities in the past few decades in a transforming environment.

On a practical level, intelligence work has always been easily defensible in intelligence and policy circles (Buchan, 2015, p. 174). The trade performs a crucial job, the outcome of which feeds directly into national security and

strategic agendas, and is thus tolerated as a necessary evil, something to be mitigated rather than prohibited when a slip-out occurs (Chesterman, 2006, p. 1098). Yet, for international lawyers intelligence practices and international law, and espionage in particular, have always had a tedious relationship. The lack of codification of intelligence practices beyond the national level has led different commentators to allocate espionage different standing within the international legal order. To put in a nutshell, there are roughly four main understandings of espionage's status as far as international lawyers are concerned: Espionage is illegal (Buchan, 2016; Wright, 1962), legal (Demarest, 1995; Smith, 2006; Lubin, 2016), neither (Baker, 2003; Brown & Metcalf, 2014; Parks, 1990), or sometimes illegal and sometimes not (Deeks, 2016; Forcese, 2011, 2016).

Changes in the international landscape brought about by the post-Cold War era complicated further the legal classification of espionage—lessons on intelligence activities learnt in a bipolar world order turned out difficult to translate into the new, multipolar context. Thus, already in the early 1990s, commentators spoke of changed intelligence norms (Demarest, 1995, p. 321) and sought for interpretations and additions to the international law framework to accommodate espionage's evolving normative status. It should be noted, however, that espionage in that early post-Cold War period meant exclusively the intelligence collection accomplished by human agents (Buchan, 2018, p. 3; Warner & Andregg, 2007, p. 28). The latter implies a clandestine targeted operation infiltrating a particular setting in order to obtain specific source(s) of information. TeDi's analysis illustrates how both the term "espionage" and the practice of espionage have evolved in the digital age: One speaks of cyber espionage when a cyber exploitation tool targets a particular system/network, scanning for precise bits of information. Although the underlying technical framework bears resemblance with the vast collection of signals intelligence—after all, both signals intelligence and cyber espionage target information available at and enabled by ICTs—the decisive aspect to keep them apart is the nature of data collection. Cyber espionage is targeted, while signals intelligence is indiscriminate (bulk) information gathering.

Consequently, the idea that the intelligence community creates and abides by its own normative framework is certainly not new. In the early to mid-2000s, especially in relation to security alliances in the War on Terror, commentators were mostly concerned with emerging dynamics of information use and sharing (Chesterman, 2006, p. 1099) among foreign intelligence agencies and the normative message portrayed thereby. Those concerns prevailed even past the Snowden revelations when states and other stakeholders embarked on individual protection campaigns from the too eager eye of foreign intelligence. Intelligence mishaps were mitigated by means of oversight (and privacy) regulation to push back on the now emerging cyber

intelligence norms. Yet one obvious aspect escaped the analytical hype for the most part—the ubiquity of intelligence presence in the cyber domain and its implications for the domain’s future development and regulation. Thus, while the overall damage control strategy put in place redress mechanisms dealing with the pervasiveness of intelligence methods, the changes in intelligence orientation gradually redefined intelligence paradigms (Loleski, 2019, p. 113) and boosted the developing intelligence norms further.

The latter is evidenced by the extraordinary range of intelligence tools leaked in the past years (Buchan, 2018, p. 4). Although initial coverage focused primary on individuals in active state duty and institutional targets—Chancellor Angela Merkel, the Pope, EU officials, and UNICEF, to name just a few (Buchan, 2018)—TeDi’s analysis and the examples of cyber operations in the preceding sections show the other side of the coin. Intelligence capabilities have proliferated in collecting data in bulk—by tapping directly into the Internet backbone, that is the fiber optic cables undersea (Paganini, 2014)—in tailored cyber espionage operations against private and public parties, (Argaman & Siboni, 2014; Boeke & Broeders, 2018; Kittichaisaree, 2017), as well as in cyber tools affecting hospitals, plant production sites, oil companies, and others, which have the capacity to induce indiscriminate damage (Shane, Perlroth, & Sanger, 2017). Combined with traditional intelligence features such as low political visibility and secrecy, said proliferation has effectively granted intelligence actors a wide margin of discretion when it comes to picking intelligence targets, altering ICT systems, creating technological tools, and others, without necessarily going through the foreign offices.<sup>1</sup>

The above developments have coincided with the global effort to regulate and promote responsible (state) behavior in cyberspace for a reason; the omitted calculation of the intelligence agencies’ role therein as well. To accommodate the latter requires a regulatory approach that apprehends the changed actor constellation (Treib, Bähr, & Falkner, 2007, p. 3) in a manner that already acknowledges the domain’s multi-layered and multi-actor interactions (Van den Berg et al., 2014) during both the formulation and the implementation of cyber norms and related policies.

Public administration and governance have a long tradition of questioning the aptitude of the “do-it-alone” state/government perspective (Kooiman, 2003) of governing. When moving away from the latter model, the work of Kooiman (1993, 1999) and Rhodes (2007) on networked governance is of particular interest. The essence of Kooiman’s argument is that governance of modern societies is a mixture of governing efforts by a wide range of actors—public, private, sub-state, and supra-state ones. Traditional government structures are not obsolete (1999, p. 73), but rather facilitators, partners in a governing process, in which no single actor or entity has the capacity to deal with problems (1993, p. 4) by itself in an ever growing societal diversity

and complexity. Rhodes for his part refers to the phenomenon as “the hollowing out of the state” (2007, p. 1249)—erosion of the state from above through international interdependence; from below by markets and networks; and sideways from agencies. Put differently, there is no such thing as a coherent nation state, but a network of actors that promote governance instead of government. Consequently, contemporary regulation efforts need to factor in the roles of previously uninvolved (or even ambiguous (Erskine & Carr, 2016, p. 97)) societal actors, their changing relationships with others and among each other (Kooiman, 1999, p. 73), and be weary of the particularities of the respective context of regulation. Naturally, frameworks and arrangement are to vary sector by sector (Kooiman, 2003, p. 3).

This concept of governance is deemed here preferable as it manages to grasp the particularities of our interconnected society and to better identify the relevant agents that assume but also discharge norm-setting responsibility. Not surprisingly, its rationale resonates to a large extent with the conceptualization of cyberspace as consisting of different layers, and corresponds in particular to the governance layer of cyberspace (Van den Berg et al., 2014). Topping the basic technology layer and the subsequent socio-technical layer, the governance layer is understood to consist of a variety of actors interacting in complex ways (Van den Berg et al., 2014). The views of Kooiman and Rhodes thus do justice to the features of the cyber domain, and render it possible to look at the sub-state level to isolate, among other, state agencies as separate, relevant governing, norm-setting and norm-propelling entities.

This is of particular value for the purposes of the present paper, as it allows to look at the NSA—the creator of TeDi—but also at other agencies as separate actors whose practices and their corresponding implications for the debate on (cyber)governance in general, and on cyber norms in particular, can be studied. What is more, adopting such an understanding does not dismiss the relevance of state and non-state actors in the process. It simply accounts for the fact that as cyberspace crosses national boundaries, so too conceptual boundaries have to be crossed to cope with the domain’s regulatory complexity. In addition, the fact that this mode of governance is implemented by interactions among different entities prepares the ground for the further zooming into other relevant interactions—those within the intelligence community. Thus, by regarding intelligence agencies as (international) actors and norm-setters in cyberspace, the formation and functioning of practices that accompany norm-formation in specific sectors can be traced, and better comprehended.

### **Norm-setting behavior**

Having discussed why and how to conceptually accommodate the intelligence agencies as actors in the debate on global cyberspace regulation, this section

turns to map their actual norm-propelling behavior. It thus draws on existing norms scholarship and on TeDi's forensic analysis to pinpoint a norm on cyber espionage. The latter evidences a profound shift in the contemporary intelligence context and urges re-consideration of contemporary norm drafting approaches.

How norms come into being has been theorized across a number of disciplines. Accordingly, the concept of a norm and a norm's life cycle (Erskine & Carr, 2016, p. 92; Finnemore & Sikkink, 1998, p. 895) are relatively well established. The predominant understanding in political and social science is that a norm refers to collective expectations for the appropriate behavior of actors with a given identity (Katzenstein, 1996, p. 5). Said concept frames earlier studies of political and normative change (Finnemore, 1996, p. 22; Finnemore & Sikkink, 1998, p. 891), and largely informs the cyber norms debate as well (Finnemore & Hollis, 2016, p. 438; Hollis, 2017, p. 4). Thus, to claim the existence of the alleged cyber espionage norm, we need to establish the quality of its four building blocks—behavior, identity, propriety, and expectations (Finnemore & Hollis, 2016, pp. 438–444; Hollis, 2017, p. 4), and to decipher their underlying values, standards, and codes of conduct (Erskine & Carr, 2016, p. 93).

The identity of the relevant actors—the intelligence agencies which allegedly generate and abide by the norm—was already elaborated upon above. Thus, for the sake of brevity, this section focuses on outlining the behavior that is deemed norm-constitutive, its appropriateness and the expectations that stem from it.

Behavior describes particular actions, a regularized practice (Finnemore & Sikkink, 1998, p. 894), prescribed by the norm for the respective community (Finnemore & Hollis, 2016, p. 440). As norms leave only indirect evidence of their existence (Finnemore & Sikkink, 1998, p. 892), one is prompt to engage with the trail of interactions between actors to identify standardized behavior. Indications of norm-conforming behavior can be seen, for instance, when a practice is taken for granted (Finnemore & Sikkink, 1998, p. 892). This usually points to an internalization of a behavioral pattern (Erskine & Carr, 2016, p. 91) that is seldom contested (Finnemore, 1996, p. 23). Propriety on its turn is the grounds on which a behavior is designated appropriate or not. Here multiple factors—culture, professional standards, politics, law, and others—can be at work at the same time (Finnemore & Hollis, 2016, p. 441) and have an impact on recognizing something as norm-conform and thus proper. Last but not least, a few words on collective expectations: those are the ones that underpin the social and intersubjective character of norms. This final ingredient attests that a community shares an understanding about the propriety of a certain behavioral practice. The extent of that intersubjectivity can and usually do vary, especially when multiple norms clash in the same normative context (Finnemore & Hollis, 2016, p. 443).

TeDi offers an example of such an internalized behavior—one that is routinely carried out, accompanied by standard operator interventions. While it is true that the available forensic information refers to NSA conduct only, the fact that the agency scans for a list of long-term running standardized threats, corroborates this point for other foreign intelligence agencies as well. This reasoning is further supported by the detailed behavior instructions software operators ought to abide by when they encounter foreign actors on targeted systems (Bencsáth, 2018, p. 4). The instructions mandate to avoid open confrontations and in a sense to “tiptoe” around other operators. The presence of foreign counterparts is thus a given and explicitly factored in official proceedings with a *laissez-faire* attitude. This means, in practice, that not only it is possible to find multiple APTs on high value systems (Zetter, 2018), but that the NSA takes it for granted that other intelligence parties are there as well and will conduct themselves in a similar manner.

This mindset is particularly relevant, as without anticipating (at least a part of) the intelligence community to reciprocate TeDi’s behavior and to do so out of a communal belief in its propriety, there can be no norm. Consequently, we can speak of a community-encompassing behavioral standard around which the NSA and other agencies structure cyber espionage activities and thus abide by. If there would not be a norm relating thereto, there would be no need for the operators of TeDi to conduct themselves according to guidelines created to cushion online encounters. They would simply act in a unilateral way without due regard to others’ activities and views thereon. The cyber norm on espionage is thus evidenced by its careful yet routine behavioral operationalization. As for its propriety, it seems that intelligence culture and influential professional standards are the main sources of the community understanding that said behavior is proper. In that regards it is not unusual that intelligence culture is precisely the one undermining the normative claim at hand. In cyberspace, culture is often the one substantiating normative propositions (Finnemore & Hollis, 2016, p. 442).

Ongoing academic and political debates about cyber espionage that problematize it or even “red-flag” it on the cyber security agendas of both individual states and the international community as a whole do not contradict the above finding. After all, norms emerge in spaces that are highly contested by other normative perceptions and interests (Finnemore & Sikkink, 1998, p. 897). These clash with each other (Finnemore & Sikkink, 1998, p. 897), while striving to create alternative perceptions of both interests and appropriateness. Thus, it is not uncommon that what one community establishes as appropriate, is perceived as inappropriate or even wrong in another context by another group of actors. Cyberspace is by no means a normative vacuum (Finnemore & Hollis, 2016, p. 444).

So why would such an extensive attention to a cyber espionage norm matter? After all, everybody knows that spies spy, that is what intelligence



agencies are created for and bound to do. For one, because at this stage of the debate the two conventional remedies—“Don’t get caught with your hands in the honey pot” and “It wasn’t me” (Demarest, 1995, p. 340)—will simply not do the trick anymore. Intelligence tools that are now in the open not only confirm the old stand-by “Everybody does it,” they provide us with unique insights into the level of awareness intelligence agencies have of each other’s practices and how they operate as a norm-abiding community. This is a unique opportunity to see through the eyes of the agencies (Greenberg, 2018a) themselves.

Further, and more importantly, it matters because TeDi and its SIG list do not just exemplify any norm, but a changed fundamental, constitutive norm; a norm that has elevated the intelligence agencies to autonomous actors whose rules have implications for the rest of the international community as well. The cyber espionage norm portrays ideally the profound environmental change experienced by intelligence agencies over the last two decades, and especially so with regard to foreign intelligence. From discretely entering, snooping around and leaving the premises, espionage has evolved into special units’ breaking and entering to live on the networks (National Security Agency/Central Security Service, 2000). This direct data extraction (Loleski, 2019, p. 117) or active signals intelligence (Hayden, 2017; Warner, 2017, p. 23) as others call it, has redefined the cyber domain as a mere component of signals intelligence (Loleski, 2019, p. 117). Such a take on cyber operations challenges the way one thinks of cyber regulation, international law and cyber norms all together.

Norms governing online behavior are not always clear (Finnemore & Hollis, 2019, p. 22), nor are their consequences always accounted for (Hollis, 2017, p. 23)—certainly less so, when the actors behind them never intended to be in the public eye in the first place. Yet, the improved visibility of intelligence activities and their scope have made it evident that there is an overt normative context within which intelligence actors operate internationally. Another aspect is also clear—that the purposes for which the foreign intelligence apparatus is used have also changed. From a normative perspective a shift, a movement is always welcome. After all, when it comes to norm construction, the process itself is the product (Hollis, 2017). When it comes to global cyber regulation, however, such findings put the contradictory relationship of international law and espionage on the spot.

## Conclusion

This article set out to map the rather (at least at first sight) counter-intuitive cyber norm-setting capacity of contemporary intelligence and security agencies. Though the idea of community-developed and implemented



norms is not new, what makes the case of the intelligence agencies in cyberspace unusual is that their norms are showing significant implications for actors outside the intelligence community as well. This article thus points to a fundamental change in the contemporary intelligence landscape—one that has converted cyberspace into a mere component of foreign intelligence operations—that requires its incorporation into further conceptualizations of the global cyberspace regulation agenda.

This article first revisited forensic insights from the scientific report authored by the Budapest-based CrySyS team dealing with the NSA cyber exploitation tool TeDi. The latter gave unique insights into how intelligence actors interact with and track each other online. The article then examined TeDi's features in combination with the concept of networked governance, allowing to factor in cyberspace's de-centralized layers and the actors interacting therein, to highlight the intelligence agencies' actorship characteristics. It thereby called for the consideration of norms' foundational practices already at the micro level—as they are being implemented by the actors who create them within their respective communities—rather than considering them from the top or macro level where they are often dealt with in “should” terms. This approach does not stand in opposition to what has been done so far in academic writings. It is complementary, not competing, as it is concerned with pointing out that current cyberspace regulation strategies do not have the capacity to explain all phenomena and to comprehensively address regulation gaps that result from them. The latter is especially true in the challenging foreign intelligence context, which is evolving at a quick pace and not well understood by outsiders.

The article then took to outlining behavioral patterns portrayed by TeDi that evidence a particular norm on cyber espionage. Hence, the article argued that cyber intelligence conduct should be explicitly calculated into ongoing cyber norm-making efforts, be those part of the UN GGE process or other international consortia. After all, when attempting to clarify the rules and norms of cyberspace, one might as well start with the already existing ones that are being applied in particular contexts on daily basis.

As a final note it should be emphasized that the article addressed solely the norm-setting capacity of intelligence actors. How intelligence norms, once developed, are being propagated and picked up by other non-intelligence actors as a result of effective norm-entrepreneurship is a different issue. This differentiation has necessarily to do with the fact that appreciating the form and function of intelligence norms is rather a technical task, connected to but not identical with the wider strategic context responsible for further norm-promotion, adoption or even codification in binding instruments. The underlying rationale of such an approach is to illustrate the importance of norm-setting, which if improperly handled, can turn norm entrepreneurial

endeavors into the empty shells of policy statements. The author thus hopes to have demonstrated utility.

## Note

1. Of course, when it comes to diplomatic risks, intelligence operations are closely coordinated with the respective foreign affairs authorities. This, however, is often not the case with cyber operations, in which the agencies have a large margin of appreciation.

## Acknowledgements

This paper builds upon the conference paper “Intelligence agencies as international norm-setters,” presented on September 25, 2018, at the State of the Art of Cybersecurity and Cyberconflict Research Conference organized by ETH in Zurich.

## Disclosure statement

No potential conflict of interest was reported by the author.

## Notes on contributor

**Ilina Georgieva** is a Ph.D. candidate of The Hague Program for Cyber Norms. In her research, she is focusing on the capacity of intelligence agencies to propagate cyber norms by means of their conduct in cyberspace, and to thus shape the international community’s perception of what is normal in cyberspace. For that purpose she investigates the agencies’ normative power by looking into their practice of foreign bulk data collection. Prior to joining the Institute of Security and Global Affairs, Georgieva served as a researcher on the Sweetie 2.0 Project at eLaw, the Center for Law and Digital Technologies at Leiden University. Her research encompassed a comparative legal study concerning the trans-border investigation of webcam child sex tourism. While at eLaw, she also co-authored a comparative study on data protection policies in eight different EU jurisdictions.

## ORCID

Ilina Georgieva  <http://orcid.org/0000-0002-3747-191X>

## Reference List

- Abbott, K. W., & Snidal, D. (2000). Hard and soft law in international governance. *International Organization*, 54, 421–456. doi:10.1162/002081800551280
- Argaman, S., & Siboni, G. (2014). Commercial and industrial cyber espionage in Israel. *Military and Strategic Affairs*, 6, 43–58.
- Baker, C. D. (2003). Tolerance of international espionage: A functional approach. *American University International Law Review*, 19, 1091–1113.

- Ball, J., Borger, J., & Greenwald, G. (2013). Revealed: how US and UK spy agencies defeat internet privacy and security. *The Guardian*. Retrieved from <https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>
- Bencsáth, B. (2018). *Territorial Dispute – NSA's perspective on APT landscape. Technical report with the analysis team of Ukatemi and CrySys Lab*. Retrieved from [https://www.crysys.hu/files/tedi/ukatemicrysys\\_territorialdispute.pdf](https://www.crysys.hu/files/tedi/ukatemicrysys_territorialdispute.pdf)
- Bethlehem, D. (2012). The secret life of international Law. *Cambridge Journal of International and Comparative Law*, 1, 23–36. doi:10.7574/cjicl.01.01.1
- Biddle, S. (2016). The NSA Leak Is Real, Snowden Documents Confirm. *The Intercept*. Retrieved from <https://theintercept.com/2016/08/19/the-nsa-was-hacked-snowden-documents-confirm/>
- Boeke, S., & Broeders, D. (2018). The demilitarisation of cyber conflict. *Survival*, 60, 73–90. doi:10.1080/00396338.2018.1542804
- Broeders, D., Boeke, S., & Georgieva, I. (2019). Foreign intelligence in the digital age. Navigating a state of 'unpeace'. The Hague Program For Cyber Norms Policy Brief. September 2019.
- Brown, G. D., & Metcalf, A. O. (2014). Easier said than done: Legal reviews of cyber Weapons. *Journal of National Security Law and Policy*, 7, 115–138.
- Buchan, R. (2015). Cyber espionage and international law. In N. Tsagourias, & R. Buchan (Eds.), *Research handbook on international law and cyberspace* (pp. 168–189). Cheltenham: Edward Elgar Publishing.
- Buchan, R. (2016). The international regulation of cyber espionage. In A.-M. Osula, & H. Rõigas (Eds.), *International cyber norms: Legal, policy and industry perspectives* (pp. 65–86). Tallinn: NATO CCD COE Publications.
- Buchan, R. (2018). *Cyber espionage and international law*. Oxford: Hart Publishing.
- CCDCOE. (2017). Tallinn Manual Process. Retrieved from <https://ccdcoe.org/research/tallinn-manual/>
- CFR - Council on Foreign Relations. (2019). Cyber Operations Tracker. Retrieved from <https://www.cfr.org/interactive/cyber-operations>
- Chesterman, S. (2006). The spy who came in from the cold war: Intelligence and international law. *Michigan Journal of International Law*, 27, 1071–1130. doi:10.1093/jiip/jpl178
- Committee on the Formation of Customary (General) International Law. (2000). *Final Report of the Committee - Statement of Principles Applicable to the Formation of General Customary International Law*. Retrieved from <https://www.law.umich.edu/facultyhome/drwcsebook/Documents/Documents/ILAReportonFormationofCustomaryInternationalLaw.pdf>
- Deeks, A. (2016). Confronting and adapting: Intelligence agencies and international law. *Virginia Law Review*, 102, 599–685.
- Demarest, G. B. (1995). Espionage in international law. *Denver Journal of International Law and Policy*, 24, 321–348.
- Engelkamp, S., & Glaab, K. (2015). Writing norms: Constructivist norm research and the politics of ambiguity. *Alternatives: Global, Local, Political*, 40, 201–218. doi:10.1177/0304375415612270
- Erskine, T., & Carr, M. (2016). Beyond “quasi-norms”: The challenges and potential of engaging with norms in cyberspace. In H. Osula & A.-M. Rõigas (Eds.), *International cyber norms: Legal, policy & industry perspective* (pp. 87–109). Tallinn: NATO CCD COE Publications.
- Executive Office of the President of the United States. (2011). *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked*

- World. Retrieved from [https://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf)
- Farrell, H. (2015). *Promoting Norms for Cyberspace*. Retrieved from [https://www.cfr.org/sites/default/files/pdf/2015/03/Norms\\_CyberBrief.pdf](https://www.cfr.org/sites/default/files/pdf/2015/03/Norms_CyberBrief.pdf).
- Farrell, H., & Glaser, C. L. (2017). The role of effects, salencies and norms in US Cyberwar doctrine. *Journal of Cybersecurity*, 3, 7–17. doi:10.1093/cybsec/tyw015
- Finnemore, M. (1996). Defining state interests. In *National interests in international society* (pp. 1–33). Ithaca, NY: Cornell University Press.
- Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, 110, 425–479. doi:10.5305/amerjintlaw.110.3.0425
- Finnemore, M., & Hollis, D. B. (2019). *Beyond naming and shaming: Accusation and International Law in Cybersecurity* (Temple University Legal Studies Research Paper No. 2019-14). doi:10.2139/ssrn.3347958
- Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, 52, 887–917. doi:10.1162/002081898550789
- Forcese, C. (2011). Spies without borders: International law and intelligence collection. *Journal of National Security Law & Policy*, 5, 179–210.
- Forcese, C. (2016). Pragmatism and principle: Intelligence agencies and international Law. *Virginia Law Review Online*, 102, 67–84.
- Foreign & Commonwealth Office and The Rt Hon William Hague. (2011). London Conference on Cyberspace: Chair's statement - GOV.UK. Retrieved from <https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement>
- GCSC. (2016). Global Commission on the Stability of Cyberspace. Retrieved from <https://cyberstability.org/>
- Greenberg, A. (2018a). Spy v. Spy: An NSA leak reveals the agency's list of enemy hackers. *Wired*. Retrieved from <https://www.wired.com/story/nsa-leak-reveals-agency-list-enemy-hackers/>
- Greenberg, A. (2018b). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. Retrieved from <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
- Grigsby, A. (2017). The end of cyber norms. *Survival*, 59, 109–122. doi:10.1080/00396338.2017.1399730
- Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53, 1155–1175. doi:10.1111/j.1468-2478.2009.00572.x
- Hayden, M. V. (2017). *Playing to the edge: American intelligence in the age of terror*. London: Penguin.
- Henriksen, A. (2019). The end of the road for the UN GGE process: The future regulation of cyberspace. *Journal of Cybersecurity*, 5, 1–9. doi:10.1093/cybsec/tyy009
- Hollis, D. B. (2017). China and the U.S. Strategic Construction of Cybernorms: The Process is the Product. *Aegis Paper Series No. 1704*, 1–24. Retrieved from <https://www.hoover.org/research/china-and-us-strategic-construction-cybernorms-process-product>
- HPCN. (2018). The Hague program for Cyber Norms. Retrieved from <https://www.thehaguecybern timer.nl>
- Hurwitz, R. (2014). The play of states: Norms and security in cyberspace. *American Foreign Policy Interests*, 36, 322–331. doi:10.1080/10803920.2014.969180
- Kaspersky Lab. (2019). BlackEnergy APT Attacks | What is BlackEnergy? *Kaspersky Lab*. Retrieved from <https://www.kaspersky.com/resource-center/threats/blackenergy>

- Katzenstein, P. J. (1996). Introduction: Alternative perspectives on national security. In P. J. Katzenstein (Ed.), *The culture of national security: Norms and identity in world politics* (pp. 1–32). New York: Columbia University Press.
- Kittichaisaree, K. (2017). Cyber espionage. In *Public international Law of cyberspace* (pp. 233–262). Cham: Springer.
- Kooiman, J. (1993). Social-political governance: Introduction. In J. Kooiman (Ed.), *Modern governance: New government-society interactions* (pp. 1–6). London: SAGE Publications.
- Kooiman, J. (1999). Social-political governance. *Public Management Review*, 1, 67–92. doi:10.1080/14719037800000005
- Kooiman, J. (2003). *Governing as governance*. London: Sage.
- Krook, M. L., & True, J. (2012). Rethinking the life cycles of international norms: The United Nations and the global promotion of gender equality. *European Journal of International Relations*, 18, 103–127. doi:10.1177/1354066110380963
- Langevin, J. R., Mccauley, M. T., Charney, S., & Lewis, J. A. (2008). *Securing cyberspace for the 44th Presidency: A report of the CSIS Commission on cybersecurity for the 44th Presidency*. Washington: Center for Strategic and International Studies.
- Loleski, S. (2019). From cold to cyber warriors: The origins and expansion of NSA's tailored Access operations (TAO) to shadow brokers. *Intelligence and National Security*, 34, 112–128. doi:10.1080/02684527.2018.1532627
- Lubin, A. (2016). Espionage as a Sovereign right under international law and its Limits. *ILSA Quarterly*, 24, 22–28.
- Macák, K. (2017). From cyber norms to cyber rules: Re-engaging states as law-makers. *Leiden Journal of International Law*, 30, 877–899. doi:10.1017/s0922156517000358
- McKay, A., Neutze, J., Nicholas, P., & Sullivan, K. (2014). *International cybersecurity norms: Reducing conflict in an Internet-dependent world*. Microsoft. Retrieved from <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA>
- Microsoft. (2016). *International Cybersecurity Norms*. Retrieved from <https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/>
- Nakashima, E., & Timberg, C. (2017). NSA officials worried about the day its potent hacking tool would get loose. Then it did. *The Washington Post*. Retrieved from <https://cyber-peace.org/wp-content/uploads/2017/05/NSA-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose.-Then-it-did.pdf>
- National Security Agency/Central Security Service. (2000). *Transition 2001*. Retrieved from <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB24/nsa25.pdf>
- Paganini, P. (2014). RAMPART-A allows NSA to tap into fiber optic cables world-wide. *Security Affairs*. Retrieved from <https://securityaffairs.co/wordpress/25962/intelligence/rampart-nsa-program.html>
- Parks, H. W. (1990). The international law of intelligence collection. In J. N. Moore, & R. F. Turner (Eds.), *National security Law* (pp. 433–434). Durham, North Carolina: Carolina Academic Press.
- Perina, A. H. (2015). Black holes and open secrets: The impact of covert action on international law. *Columbia Journal of Transnational Law*, 53, 507–583.
- Peterson, A. (2014). The Sony Pictures hack, explained. *The Washington Post*. Retrieved from <https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/>
- Rhodes, R. A. W. (2007). Understanding governance: Ten years on. *Organization Studies*, 28, 1243–1264. doi:10.1177/0170840607076586

- Sanger, D. E. (2016). 'Shadow Brokers' Leak Raises Alarming Question: Was the N.S.A. Hacked? *The New York Times*. Retrieved from <https://www.nytimes.com/2016/08/17/us/shadow-brokers-leak-raises-alarming-question-was-the-nsa-hacked.html>
- Shane, S., Perlroth, N., & Sanger, D. E. (2017). Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core. *The New York Times*. Retrieved from <https://www.nytimes.com/2017/11/12/us/nsa-shadow-brokers.html>
- Shaw, M. N. (2014). *International law* (7th ed.). Cambridge: Cambridge University Press.
- Siemens, Airbus, IBM, Allianz, Conference, M. S., SGS, ... T-Mobile. (2018). *Charter of Trust: For a secure digital world*. Retrieved from <https://assets.new.siemens.com/siemens/assets/public/1560760957.55badda4-4340-46d3-b359-f570e7d1f4c2.chart-er-of-trust-presentation-en.pdf>
- Smith, B. (2017). Transcript of Keynote Address at the RSA Conference 2017 - The Need for a Digital Geneva Convention. *Microsoft Corporation*, 1–15. Retrieved from <https://mscorpmedia.azureedge.net/mscorpmedia/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf>
- Smith, J. H. (2006). Keynote address. *Michigan Journal of International Law*, 28, 543–552.
- Stevens, T. (2012). A cyberwar of ideas? Deterrence and norms in cyberspace. *Contemporary Security Policy*, 33, 148–170. doi:10.1080/13523260.2012.659597
- Stout, M., & Warner, M. (2018). Intelligence is as intelligence does. *Intelligence and National Security*, 33, 517–526. doi:10.1080/02684527.2018.1452593
- Tikk, E., & Kerttunen, M. (2017). *The Alleged Demise of the UN GGE: An Autopsy and Eulogy*. 1–41. Retrieved from <http://cpi.ee/wp-content/uploads/2017/12/2017-Tikk-Kerttunen-Demise-of-the-UN-GGE-2017-12-17-ET.pdf>
- Tikk-Ringas, E. (2017). International cyber norms dialogue as an exercise of normative power. *Georgetown Journal of International Affairs*, 17(3), 47–59. doi:10.1353/gia.2016.0036
- Treib, O., Bähr, H., & Falkner, G. (2007). Modes of governance: Towards a conceptual clarification. *Journal of European Public Policy*, 14, 1–20. doi:10.1080/1350176060061071406
- United Nations. (2010). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security A/65/201*. Retrieved from <https://undocs.org/A/65/201>
- United Nations. (2011). *Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. Retrieved from <https://www.un.org/disarmament/publications/library/66-ga-ga-sc/>
- United Nations. (2015). *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General*. Retrieved from <https://digitallibrary.un.org/record/786846>
- Van den Berg, J., Van Zoggel, J., Snels, M., Van Leeuwen, M., Boeke, S., Van de Koppen, L., ... De Bos, T. (2014). On (the Emergence of) Cyber Security Science and its Challenges for Cyber Security Education. *Proceedings of the NATO IST-122 Cyber Security Science and Engineering Symposium*, 13–14. Retrieved from <https://www.csacademy.nl/images/MP-IST-122-12-paper-published.pdf>
- Warner, M. (2017). Intelligence in cyber-and cyber in intelligence. In G. Perkovich, & A. E. Levite (Eds.), *Understanding cyber conflict: Fourteen Analogies* (pp. 17–29). Washington, DC: Georgetown University Press.

- Warner, M., & Andregg, M. (2007). The study of intelligence/ sources and methods for the study of intelligence/intelligence ethics. In L. K. Johnson (Ed.), *Handbook of intelligence studies* (pp. 17–63). London: Routledge.
- Wright, Q. (1962). Espionage and the doctrine of non-intervention in international affairs. In R. J. Stanger (Ed.), *Essays on espionage and international Law* (Vol. 3, pp. 3–28). Columbus: Ohio State University Press.
- Zetter, K. (2010). Google Hack Attack Was Ultra Sophisticated, New Details Show. *Wired*. Retrieved from <https://www.wired.com/2010/01/operation-aurora/>
- Zetter, K. (2014). DarkHotel: A Sophisticated New Hacking Attack Targets High-Profile Hotel Guests. *Wired*. Retrieved from <https://www.wired.com/2014/11/darkhotel-malware/>
- Zetter, K. (2018). Leaked Files Show How the NSA Tracks Other Countries' Hackers. *The Intercept*. Retrieved from <https://theintercept.com/2018/03/06/leaked-files-show-how-nsa-tracks-other-countries-hackers/>
- Ziolkowski, K. (2013). Peacetime cyber espionage: New tendencies in public international law. In K. Ziolkowski (Ed.), *Peacetime regime for state activities in cyberspace: International law, international relations and diplomacy* (pp. 425–464). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.