The Power of Norms Meets Normative Power: On the International Cyber Norm of Bulk Collection, the Normative Power of Intelligence Agencies and How These Meet

Ilina Georgieva

Cite as: Georgieva, Ilina. 2020. "The Power of Norms Meets Normative Power: On the International Cyber Norm of Bulk Collection, the Normative Power of Intelligence Agencies and How These Meet." In *Governing Cyberspace: Behavior, Power, and Diplomacy*, edited by Dennis Broeders and Bibi van den Berg, 227-242. London: Rowman & Littlefield International.

More information about the book and The Hague Program for Cyber Norms is available on:

www.thehaguecybernorms.nl

Chapter 11

The Power of Norms Meets Normative Power

On the International Cyber Norm of Bulk Collection, the Normative Power of Intelligence Agencies and How These Meet

Ilina Georgieva

The world has been witnessing unprecedented intelligence revelations ever since the whistleblower Edward Snowden took on his role in the summer of 2013. What started off as an affair concerning the National Security Agency (NSA) and the Government Communications Headquarters (GCHQ), quickly evolved in a debate that transcended the Anglo-American context of security breaches and fundamental rights intrusions, and established itself as a long-lasting point on the policy agendas of most liberal states. Governments and agencies caught in the act had to regroup to regain public trust, and to do so quickly. What followed was a wave of inquiries (UK 2015; DoD 2013) and committees (Bundestag 2014), further disclosures induced by government officials to strengthen counter-narratives (Schulze 2015, 211), eventually crowned with the adoption of legislation amendments concerning the intelligence sector. In other words, regulation was called to the rescue in an intelligence crisis that seemed omnipresent. However, as limitations proved difficult (Boeke 2017) or even impractical, the formal re-evaluation of the controversial intelligence methods led to their (renewed) codification.

At the same time, the increasing legalization of intelligence practices, a phenomenon sometimes referred to as "intelligence legalism" (Schlanger 2015), has been gaining a foothold internationally as well (Deeks 2016, 13). The taboo of talking about intelligence methods and rationales has been lifted, and with it a possibility has arrived to further evaluate them and their impact. In light of this, international actors of all shapes and sizes have been

increasingly concerned with the systematic application of (binding and non-binding) norms to intelligence practices (Deeks 2016, 17). While states, for instance, used to only occasionally make use of international rules to contest other states' intelligence mischief, international law (and international human rights law in particular) (Cole 2013; Borger 2013; Gallagher 2013; Scheinin 2014) has been enjoying quite the comeback in recent scholarship (Buchan 2016; Kittichaisaree 2017). Further, the United Nations Group of Governmental Experts (UNGGE) cyber-norms process (United Nations 1999), although indirectly related to intelligence activities, paved the way for further exploration of international norms applicable to the world's second oldest profession and its particularities in cyberspace. Scholars have been thus piecing together the intelligence practices puzzle in the cyber domain, putting forward the existence of a cyber norm on counterespionage and a cyber norm prohibiting economic espionage (Libicki 2017), to name just a few.

This chapter aims to add to the cyber-norms scholarship by tracing the evolution of an international cyber norm on *foreign* bulk data collection (as opposed to data collection by means of more targeted and/or solely domestic intelligence-gathering methods). What is more, by looking into recent legislative developments in Germany, France, and the United Kingdom (UK) covering that very same intelligence methodology, the present contribution purposes to also make the case that the cyber norm on foreign bulk data collection has been already "fortified" in black letter law. This approach offers a unique opportunity to test in practice theoretical international relations (IR) concepts on international norms development and to contribute to understanding which norms become law and how exactly by exploring the connection between the proliferation of leaks and expanding legalization (Deeks 2016, 13). Last but not least, by focusing on the role of the intelligence agencies, this contribution makes the implicit claim that the debate on norms for responsible behavior in cyberspace needs to cast a wider net to consider not only top-down but also bottom-up approaches to regulation.

When speaking of the normative capacity of the intelligence agencies at hand, pinpointing the norm is only half of the story. To complete the circle, one needs to ask not only whether the agencies promote their own norms and what their impact is on (cyberspace) regulation practices, but to also look into how and what power dynamics make that possible. This chapter thus argues that the other side of the coin is the normative power (Manners 2002) of the intelligence agencies, which makes itself particularly noticeable in the "legitimacy narrative" many of the agencies adopt defending their behavior (their norms) in the post-Snowden era. What that approach accomplishes is to add to our understanding of the role of the intelligence agencies in world politics and regulation on the one hand, while contributing to the conceptions of normal in IR scholarship on the other. Thus, following Manners's conceptualization,

this chapter puts forward that to see the intelligence agencies as a normative power internationally is not "a contradiction in terms" (Manners 2002, 236), but a natural complementation of the normative process.

The main reasons for choosing to look into foreign bulk collection practices are threefold. For one, the oversea focus intends to circumvent the heated domestic debates on the checks and balances that pertain (at least to a certain extent) to rather specific domestic contexts, and have already enjoyed the attention of a number of scholars and practitioners. Second, by focusing on intelligence practices that cross national borders by default, thematic priority can be given to their relevance for both the ongoing debate on international cyber norms and for the emerging normative framework relating to cyber espionage activities. Last, bulk data is the epitome of the information age; it is what the information society in many instances thrives on, but also fears. This contribution thus takes on the opportunity to look further into the normative implications of bulk data collection.

The choice to look into the legislative developments of Germany, France and the United Kingdom bears on the following points. For one, it allows to consider both common and civil law traditions. Second, their intelligence practices (and alliances) prior to the respective intelligence reforms are well documented by primary sources, which provide for a good *ex ante—ex post* normative comparison. One can thus trace the behavioral norms the intelligence agencies were abiding by prior to the leaks, whether and how those were codified, and contrast them to current practices and legal frameworks. Further, the consideration of the normative developments in Germany, France and the United Kingdom covers a number of intelligence contexts—the United Kingdom as one of the initial driving forces behind the Five Eyes and its role as a bridge between Europe and United States; Germany, which is particularly interesting for being marked by its Stasi past and thus bound by very restrictive domestic rules regarding surveillance; and last but not least France for its rather silent development of one of the most comprehensive bulk collection mechanisms able to match the Five Eyes' ambitions long before other "elite" intelligence actors were able to do so. In addition, as the revelations and other public sources give away, all three countries are affiliated with the Five Eyes in different capacities—an interaction governed by its own diplomacy, elaborate agreements and countless treaties (Aldrich 2004, 739), creating an indisputable community culture.

The present contribution continues as follows. Section II briefly makes some terminology references and gives a few prominent examples of bulk collection which were brought to light mainly by Snowden. Section III evaluates those through the lens of IR norms scholarship to pinpoint the normativity in the agencies' behavior. Section IV presents evidence of how these methods have been fortified in legal instruments. Section V takes on the task

to trace the normative power of the intelligence agencies, followed by some concluding remarks on norms and actorship in the international system.

"TAKING THE DATA STRAIGHT FROM THE TUBES"—SOME NECESSARY CONTEXT AND TERMINOLOGY

Information collection in bulk has been central to the debate in the post-Snowden era. Naturally, definitions of the practice differ according to jurisdiction and operational context (see, for instance, Anderson 2016, 1, 2 as an example of the UK context). As a rule, bulk collection refers to an intelligence collection practice by which vast amounts of data (both content and metadata) are acquired for multiple purposes/databases without a "determinant" (Boeke 2017, 312), that is to say without aiming at a particular target, be it a geographical location or an individual. Leaving the domestic context aside, it is a standard feature of the foreign intelligence portfolio of almost any intelligence or national security agency and falls by default under its respective signals intelligence (SIGINT) capabilities. As such the practice is exercised on the premise "first collect, then select" (Boeke 2017, 312), hence the familiar-sounding metaphor of the haystack and the needle. For the sake of simplicity, the rest of this article uses "bulk data collection" or "bulk collection" as references to the collection of both content and metadata unless otherwise specified. Further, the terms are used to denote communications taking place entirely abroad, as well as communications originating/ending in the intercepting country. Consequently, *a foreign* factor is always implied.

As Snowden's revelations developed in time and scope, it became increasingly clear that a number of states had been making use of bulk collection methods (Inkster 2014, 57), either unilaterally or in peer cooperation. Valuable insights on the subject were delivered by leaks relating to the NSA's Special Source Operations (SSO) division, the crown jewel of the agency (Electrospaces 2014b). Documents pertaining to the SSO allow a rare peek into the collection practices of a number of the NSA's oversea partners including the GCHQ, the German Federal Intelligence Service (*Bundesnachrichtendienst* or BND) and the French General Directorate for External Security (*Direction Générale de la Sécurité Extérieure* or DGSE) (Electrospaces 2014a). While those liaison relationships necessarily vary in scope, durability, and authorization, they also hold commonalities when it comes to obtaining communications data in bulk. As will be explained, the common features of their operational practices are particularly telling for the intelligence community's culture and corresponding intelligence collection norms. The following examples illustrate the agencies' methodology.

Operation TEMPORA allowed GCQH to tap into the fiber optic cables that carry Internet data in and out of the United Kingdom and to collect it in bulk (MacAskill et al. 2013). By exploring the United Kingdom's unique geographical advantage and placing interceptors on the approximately 200 transatlantic cables where they come ashore (Shubber 2013), GCHQ has not only managed to secure a direct access to vast amounts of Internet data, but to do so on a scale that ranked it first in that regard among its partners the Five Eyes (Shubber 2013). The process has been facilitated by secret partnerships (voluntary or forced) with the companies that operate the cables (MacAskill et al. 2013; Obermaier et al. 2014). The legal framework for the collection appears to have been the rather broad provision of s8 RIPA 2000 (Shubber 2013). The latter allows the Foreign Secretary to issue certificates for broad interception of data categories relating to terrorism, organized crime, and so on. Inception pertains to entirely foreign communications, but also to communications whereby one of the communicating parties (either the receiver or sender) is on UK soil.

France and Germany's involvement in bulk data collection is evidenced for one thing by the RAMPART-A program (Gallagher 2014; Information.dk 2014). The leaked material pertaining to the program show that the NSA considers France and Germany "third party" countries—strategic partners outside of the Five Eyes ("second parties") providing access to transition cables and hosting equipment. The majority of the RAMPART-A missions are carried out by its partners "under the cover of an overt COMSAT effort," implying that the tapping takes place at Cold War eavesdropping stations in the intercepting countries (Gallagher 2014).

Besides additional leaks, France's engagement in bulk intelligence collection is further substantiated by a handful of investigative reports that trace the practice back to 2008 (Tréguer 2017, 2). The latter confirm the involvement of the telecommunications operators Orange and the Alcatel-Lucent group as facilitating the French DGSE's access to about two dozen undersea communications cables (Tréguer 2017, 2). Designated teams within the companies would manage the so-called landing stations, where the submarine cables touch French shore and would forward the data caught in transit to the DGSE's systems in Paris (Follorou 2014). Although lacking an actual legal framework, intelligence officials familiar with the practices have argued that the practices were not illegal, but operated rather in the grey zones of the law (Follorou and Johannès 2013).

The German BND in turn is known to have (jointly with the NSA) run the EIKONAL bulk interception program (Electrospaces 2014c)—the tapping into Deutsche Telecom cables (Biermann 2014). Sources confirm that the NSA has provided the equipment for the interception in 2003 (Electrospaces 2014c). The operation was ended in 2008, although the explanations put

forward in that regard differ. Legal authorization for the tapping of the transit cables has been provided by the G10-commission, which is required to step in once the collection of G10-data—communications data originating/ending in Germany and thus affecting nationals— is involved. Enabling statutes for fully foreign data traffic seems to have been of a lesser concern (Electrospaces 2015). EIKONAL and the agency's foreign partnerships aside, once the BND had learned how to collect Internet traffic from fiber optic cables, G10-orders were used to extract communications from about twenty-five domestic and foreign Internet service providers that made use of the DE-CIX cables positioned in Frankfurt (Electrospaces 2015).

The following section examines the examples from a normative perspective.

ALL ABOARD! GETTING ON THE NORMATIVE BANDWAGON

Norms are built by actors that have strong ideas about appropriate behavior in their community (Finnemore and Sikkink 1998, 896). What is appropriate in turn is very much linked to the role the actors in that community are performing (Sunstein 1996, 903). Norms are thus often role-specific (Sunstein 1996, 921). Consequently, evaluating the intelligence practices discussed above through the lens of IR norms literature mandates looking into them by adopting an *inwards* perspective and finding that shared understanding of the appropriateness of bulk collection within the community. Said communal perspective is particularly valuable when thinking of regulation in terms of bottom-up influences (as presently looking into the influences of substate entities on international cyber norms) that play out on the national and ultimately on the international level as well.

As the previous paragraph hints, the conventional wisdom holds that a norm is a standard of appropriate behavior for actors with a particular identity (Katzenstein 1996, 5; Finnemore and Sikkink 1998, 891; Finnemore and Hollis 2016, 438). This section thus focuses on highlighting the behavioral standards that give away the normative nature of bulk data collection for the intelligence community.

It appears that upon developing the necessary technological tools and know-how, all three agencies not only carry out extensive bulk collection programs but also operationalize the collection (their behavior) in a very similar way—by casting a wide net for foreign communications data and tapping into the accessible fiber optic cables. This *regularized*, *standardized* behavior exercised on a large-scale and without real-time constraints runs like a red thread through the examples above. The fact that the practice is not contested within the intelligence community, but seen as appropriate to serve

SIGINT purposes, encouraged through data-sharing partnerships such as the ones revealed through the NSA documents, and thus rather taken for granted with the attitude "Everybody does it," indicates norm-conforming behavior on the part of the GCHQ, the BND, and the DGSE. In IR terminology, this is one of the best examples of *norm-internalization* (Finnemore and Sikkink 1998, 895).

Note that the quality of the norm itself, that is, whether outsiders perceive it as good or bad, is not decisive, as long as the community that exercises it deems it appropriate or as inevitable to accept it (Finnemore and Sikkink 1998, 892). Put simply, the post-Snowden outrage does not abolish the bulk collection norm. It rather illustrates that the intelligence norm appeared to be in direct competition with strongly held by other actors' domestic norms on privacy and transparency of governmental agencies. Norm competition, however, is not unusual. New norms come into being in highly contested normative spaces, and while creating alternative perceptions of both interests and appropriateness, they clash with other such standards (Finnemore and Sikkink 1998, 897). Cyberspace is by no means a normative vacuum (Finnemore and Hollis 2016, 444). The extensive communication among different stakeholders upon the emergence of the bulk collection norm, accompanied by a strong and versatile rhetoric that aimed at justifying the contested behavior, on the contrary made the norm traceable and evidenced its development (Finnemore and Sikkink 1998, 892). It further means that once the leaks were out there and the necessary damage control by the use of a changed intelligence narrative and extensive communications was done, there was less fear the agencies' reputations would be additionally challenged—something Sunstein calls "social sanctions" (Sunstein 1996, 915) or in this case preempting them. Society's tolerance of the practices was secured, reputational costs lowered and thus the road ahead cleared for further fine-tuning of the bulk collection norm. That standing not only reinforced the norm within the intelligence community under scrutiny, but also paved the way for an ever-increasing number of agencies to join the bulk data collection "bandwagon" (Sunstein 1996, 930). This has had a profound knock-on effect in the legislative processes discussed below.

THE FORTIFIED CYBER NORM OF FOREIGN BULK DATA COLLECTION

A number of comprehensive intelligence reforms saw the daylight since 2013 and the ones that recently took place in France, Germany, and the United Kingdom are of particular interest here. As research into these particular legislative processes and their outcomes yielded, the contested bulk

collection—once resting on wobbly legal grounds if at all—has found its way into the statutes of these countries. The following subsection briefly presents these developments in a chronological order before moving to evaluate their meaning in the normative process.

The French Intelligence Act (FIA) (France 2015b), adopted on 24 July 2015, is the result of a long-deliberated intelligence reform.[1] The law is considered the most extensive piece of legislation relating to French surveillance practices, creating entirely new sections in the Code of Internal Security and finally legalizing already operational intelligence practices (Tréguer 2016, 2017). The FIA significantly broadens the intelligence community's collection capacities with regard to communications' content and metadata. In November of the same year, the reform was rounded off with the law on "International Surveillance" (France 2015a)—now also part of the Code of Internal Security, which focuses on international communications exclusively. The latter term is broadly defined to encompass both communications going in and out of the country (Tréguer 2016). Article L.854-2-I stipulates which network infrastructures are to be targeted for large-scale, *bulk* interception and authorizes among other things tapping into international undersea cables.

The United Kingdom followed suit by introducing the Investigatory Powers Act (IPA) in 2016 (UK 2016). The piece of legislation is understood to expand electronic surveillance powers for both law enforcement and intelligence actors. The competences outlined in the bill replace communications interception and retention powers codified by the Regulation of Investigatory Powers Act (RIPA) 2000, the Telecommunications Act (TA) 1984, the Data Retention and Investigatory Powers Act (DRIPA) 2001 and sixty-five other statutes (Anderson 2016). Further, IPA introduced new computer network exploitation powers and the ability to require retention of Internet connection records (Anderson 2016, 7). Its Part 6 and the corresponding Chapter 1 and 2 deal with bulk interception and bulk acquisition. The provisions on bulk interception replace the unclear provisions of s8 (4) RIPA and focus on "overseas-related communication," meaning communications sent or received by individuals outside the United Kingdom. The bulk acquisition powers (requiring a telecommunications provider to retain communications and disclose them pursuant to a warrant) expand the practices regulated by s94 TA that prior to the introduction of IPA was a well-kept secret (Anderson 2016, 29). The latter rules, however, affect individuals within the United Kingdom as well.

By December 2016, Germany's new surveillance laws were also on the books. The reformed BND Law introduced a number of significant new provisions with regard to the collection of foreign intelligence and international intelligence cooperation (Bundestag 2016). In its current form, the BND

Law complements the BND's collection powers by updating its *strategische Fernmeldeaufklärung* (strategic surveillance) capabilities. Adding to the agency's already existing operational powers regarding communications to and from Germany, sections 6–18 of BND Law codify for the first time the interception of communications that have both their origin and destination abroad (Wetzling 2017, 4, 5; Bundestag 2016). In that context, the amended intelligence framework covers the authorization, collection, handling, transfer and oversight of content and metadata the BND acquires in bulk. It is estimated that even prior to the legislative changes, that is to say before the existence of a proper enabling statute, the bulk collection practice made up to 90 percent of the BND's overall strategic activities (Löffelmann 2015, 1). Further, the reform allows the BND to explicitly direct intelligence operations at EU member states and EU institutions for the purpose of gathering information relevant to the country's foreign policy and security (Chase 2016).

For the sake of completeness, it should be noted that all pieces of legislation introduced above have generated significant public debates (Cobain 2018). They have further been and continue to be regularly challenged in front of judicial and other platforms by civil society groups as failing to meet international human rights and surveillance standards (ECJ 2016; Heathman 2016; Bowcott 2016; NewsWire 2018; Chase 2016).

Scholars conceptualizing the final stages of normative processes argue that institutionalization portrays the broad domestic receptiveness to a norm (Finnemore and Sikkink 1998, 906)—that the latter has been evaluated as successful (Florini 1996) to tackle ongoing societal challenges, and that putting it into binding legal instruments establishes *that* particular behavior as the credible solution for future references (Finnemore and Sikkink 1998). Thus, when prevailing norms are fortified by legal requirements (Sunstein 1996, 923), the law has a rather expressive function—it stipulates the social value of the norm encouraging it to move in a particular direction (Sunstein 1996, 953).

The above legislative summary exemplifies that the emerging bulk collection norm has reached a further phase in the normative process and it has become institutionalized (Finnemore and Sikkink 1998, 900) in specific sets of rules. The intelligence agencies studied here have thus not only developed a cyber norm on bulk collection, a norm that guides their communal practice in that regard, but have also made sure to appeal through their norm-entrepreneurial efforts (although reluctantly in the immediate post-Snowden climate) to the contemporary political context and its inherent security challenges. This has made the norm dismissal more difficult (see on the matter Keck and Sikkink 1998).

A few words need to be added here on the fact that this contribution puts forward the existence of an *international* cyber norm on bulk collection,

while drawing from *national* institutionalization examples to substantiate it. This approach goes to the core of the fundamental question where international norms come from and implicate the relationship between domestic and international norms as well. International norms must always work their way through domestic structures (Finnemore and Sikkink 1998, 893), but the process is known to work the other way around too—domestic norms also influence the emergence of widely recognized, international standards. Domestic norms are intrinsically bound with the international scene's contemporary dynamics that inevitably intervene in the local realm as well.

THE POWER OF NORMS MEETS NORMATIVE POWER

This chapter so far dealt with establishing an international cyber norm on bulk data collection developed and promoted by the intelligence agencies, a norm that later became officially codified by a number of governments placing a bet on the norm's legitimacy. It thus made a strong case for studying the international norms developed by substate agencies and their impact.

While that in itself is a curious phenomenon to trace and to learn from, it nevertheless leaves the normative puzzle at hand incomplete, as it does not tell us where that normative impact comes from. Thus, to specify the argument further, this section looks into the means and mechanisms the intelligence agencies studied here use to diffuse norms in the international system and to influence other actors.

Establishing norms for the international community implies the capacity to develop new behavioral standards and *to portray* them as appropriate *for others*. This is the mission of "norm entrepreneurs" (Sunstein 1996) put in a nutshell. Once such a pursuit has been successful, the newly established norm dictates what is *normal* in a particular context. Not that long ago, Manners studied that very capacity and came to the conclusion that "the ability to define what passes for 'normal' in world politics is extremely rich" (Manners 2002, 236). He termed it "normative power"—the power to shape what can be considered normal in international life (Manners 2002, 239)—and made a proposition that international relations are often shaped by forces beyond traditional IR power structures, by a power that works through ideas and opinions (Diez 2005, 615) using norms in instrumental ways. This notion, however, while seen as a valuable addition to the concept of soft power, has found little resonance in the analysis of power dynamics brought about by other (nontraditional) international actors, like the intelligence agencies at hand. This state of affairs is surprising, as unlike other concepts of power in IR, normative power focuses much more on cognitive processes and

ideational impacts than on institutions (Manners 2002, 239), and is as such particularly suitable to look into actors without state-like features.

The most important factor shaping the international role of the intelligence agencies as normative actors is not what they are, but what they do and what they say. As the previous sections dealt with what they do, in the following we touch upon what they say in more detail. Of course, just because a behavior can be labeled normative does not mean that all actors exercising it are normative powers. The crucial point is the ability *to frame* the responses of *others* (Kavalski 2013, 250). The post-Snowden reality delivers an example of exactly that—of the agencies' ability to change other actors' perception of, and response to, their norm of bulk data collection. The agencies (or rather their senior officers) and other related figures used a particular rhetoric to support a claim of urgency in their actions, induce credibility, and to thus normalize the practice. Covering a number of topics from the importance of counterintelligence efforts, the success of surveillance missions to track terrorists and to thwart plots (Sullivan 2013), the financial damage suffered by national security institutions that continues to grow five years after Snowden (Riechmann 2018), to even systematically downplaying the leaks where appropriate or proposing long-term privacy regulation solutions that would appeal to the public (Schulze 2015, 211), the strategy palette is rich in colors. The exact use of strategies corresponds to the escalation of the leaks (Schulze 2015, 211). Studies looking into the media coverage of the revelations confirm that the rhetoric has been successful. They illustrate that the media has largely picked up the "normalization trend" and appeared to report on bulk collection issues with reference to concerns over national security, while minimizing the attention given to individual rights (Wahl-Jorgensen, Bennett, and Taylor 2017, 740, 741). This finding feeds into Kavalski's conceptual qualification of normative power—it shows the intelligence agencies as agents of change, and what is more, is recognized as such by others (Kavalski 2013, 247). They have gained a position of credibility (Zupančič and Hribernik 2014, 79) by understanding the importance of interaction and instrumentalizing it.

In light of the above, it does not seem too far-fetched to suggest that the agencies' normative power has to do with their role and the context in which it is carried out, the particular community culture and the professional norms that result from it, supported by the successful framing of their missions and practices in the post-Snowden debates. Normative power is thus a way to conceptualize their toolbox. The latter is complemented by IR norms scholarship that tells us what is in there by studying the agencies' behavior and promoting understanding of its meaning (Finnemore 1996, 2).

CONCLUSION

This contribution embarked on a journey to make various claims. It dove into the complex debate on international cyber norms and made the case that the basis of what is deemed appropriate internationally may also arise among actors other than states—the intelligence agencies. It did so by studying their bulk collection practices, attempting to place some of Snowden's leaks in normative context and meaning. While the intelligence community did not have an interest to make its norms public, upon inevitably finding itself in the spotlight and setting irreversible precedents, it made the best of it—gained the states' support and pushed the norm on bulk data collection further. The agency's capacity to do so reflects their normative power—something assigned so far to rather state-like structures only. The chapter thus hopes to have identified various areas for future research—the involvement of substate agencies in international regulation efforts, and the basis on which such efforts may propel.

NOTE

1. Up until that date, France was one of the few Western democracies without a legal framework pertaining to the intelligence agencies. The latter's mandates were based on executive decrees and decisions in combination with other pieces of legislation such as the 1991 Wiretapping Act.

BIBLIOGRAPHY

Aldrich, Richard J. 2004. "Transatlantic Intelligence and Security Cooperation." *International Affairs* 80 (4): 731–53.

Anderson, David. 2016. "Report of the Bulk Powers Review." www.gov.uk/government/publications.

Biermann, Kai. 2014. "Daten Abfischen Mit Lizenz Aus Dem Kanzleramt." *Zeit*, 2014. https://www.zeit.de/politik/deutschland/2014-12/bnd-kanzleramt-eikonal-nsa.

Boeke, Sergei. 2017. "Reframing 'Mass Surveillance'." In *Terrorists' Use of the Internet: Assessment and Response*, edited by Maura Conway, Lee Jarvis, Orla Lehane, Stuart Macdonald, and Lella Nouri, 307–318. IOS Press.

Borger, Julian. 2013. "Brazilian President: US Surveillance a 'Breach of International Law.'" *The Guardian*, 2013.

Bowcott, Owen. 2016. "Investigatory Powers Bill Not Fit for Purpose, Say 200 Senior Lawyers." *The Guardian*, March 14, 2016.

Buchan, Russell. 2016. "The International Regulation of Cyber Espionage." In *International Cyber Norms: Legal, Policy and Industry Perspectives*, edited by Anna-Maria Osula and Henry Rõigas, 65–86. NATO CCD COE Publications.

Bundestag. 2014. "Antrag Der Fraktionen CDU/CSU, SPD, DIE LINKE. Und BUNDNIS 90/DIE GRUNEN: Einsetzung Eines Untersuchungsausschusses."

———. 2016. *Gesetz Zur Ausland-Ausland-Fernmeldeaufklärung Des Bundesnachrichtendienstes*. Bonn: Bunderstag. http://www.bundesgerichtshof.de/SharedDocs/Downloads/DE/Bibliothek/Gesetzesmaterialien/18_wp/BND-Gesetz/bgbl.pdf?__blob=publicationFile.

Chase, Jefferson. 2016. "Germany Reforms Its Main Intelligence Service." *Dw.Com*, 2016.

Cobain, Ian. 2018. "UK Has Six Months to Rewrite Snooper's Charter, High Court Rules." *The Guardian*, 2018. https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules.

Cole, David. 2013. "We Are All Foreigners: NSA Spying and the Rights of Others." Just Security, 2013.

Deeks, Ashley. 2016. "Intelligence Services, Peer Constraints, and the Law." In *Global Intelligence Oversight—Governing Security in the Twenty-First Century*, edited by Zachary K. Goldman and Samuel J. Rascoff, 3–36. New York: Oxford University Press.

Diez, Thomas. 2005. "Constructing the Self and Changing Others: Reconsidering `Normative Power Europe'." *Millennium: Journal of International Studies* 33 (3): 613–636.

DoD. 2013. "DoD Information Review Task Force-2: Initial Assessment- Impact Resulting from the Compromise of Classified Material by a Former NSA Contractor." https://nsarchive2.gwu.edu/NSAEBB/NSAEBB534-DIA-Declassified-Sourcebook/documents/DIA-48.pdf.

ECJ. 2016. Judgment in Joined Cases C-203/15 Tele2 Sverige AB v Post-och telestyrelsen and C-698/15 Secretary of State for the Home Department v Tom Watson and Others.

Electrospaces. 2014a. "NSA's Foreign Partnerships." Electrospaces.Blogpost.Com. 2014. https://electrospaces.blogspot.com/2014/09/nsas-foreign-partnerships.html.

———. 2014b. "Slides about NSA's Upstream Collection." January 17, 2014. https://electrospaces.blogspot.com/2014/01/slides-about-nsas-upstream-collection.html.

———. 2014c. "The German Operation Eikonal as Part of NSA's RAMPART-A Program." Electrospaces.Blogpost.Com. 2014. https://electrospaces.blogspot.com/2014/10/the-german-operation-eikonal-as-part-of.html.

———. 2015. "New Details About the Joint NSA-BND Operation Eikonal." Electrospaces.Blogpost.Com. 2015. https://electrospaces.blogspot.com/2015/05/new-details-about-joint-nsa-bnd.html.

Finnemore, Martha. 1996. "Defining State Interests." In *National Interests in International Society*, 1–33. Ithaca, NY: Cornell University Press.

Finnemore, Martha, and Duncan B Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110. https://doi.org/10.5305/amerjintelaw.110.3.0425.

Finnemore, Martha, and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52 (4): 887–917. http://www.jstor.org/stable/2601361.

Florini, Ann. 1996. “The Evolution of International Norms.” *International Studies Quarterly* 40 (3): 363–389.

Follorou, Jacques. 2014. “Espionnage: Comment Orange et Les Services Secrets Coopèrent.” *Le Monde*, 2014.

Follorou, Jacques, and Franck Johannès. 2013. “Révélations Sur Le Big Brother Français.” *Le Monde*, July 4, 2013. https://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html.

France. 2015a. *LOI N° 2015–1556 Du 30 Novembre 2015 Relative Aux Mesures de Surveillance Des Communications Électroniques Internationales (1)*. France: https://www.legifrance.gouv.fr/eli/loi/2015/11/30/DEFX1521757L/jo/texte.

———. 2015b. *LOI N° 2015–912 Du 24 Juillet 2015 Relative Au Renseignement (1)*. France.

Gallagher, Ryan. 2013. “After Snowden Leaks, Countries Want Digital Privacy Enshrined in Human Rights Treaty.” *Slate.Com*, September 2013. https://slate.com/technology/2013/09/article-17-surveillance-update-countries-want-digital-privacy-in-the-iccpr.html.

———. 2014. “How Secret Partnerships Expand NSA’s Surveillance Dragnet.” *The Intercept*, June 19, 2014. https://theintercept.com/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/.

Heathman, Amelia. 2016. “EU Court Deals Major Blow to UK’s Controversial Snooper’s Charter.” *WIRED*, 2016.

Information.dk. 2014. “NSA ‘Third Party’ Partners Tap the Internet Backbone in Global Surveillance Program,” June 19, 2014. https://www.information.dk/udland/2014/06/nsa-third-party-partners-tap-the-internet-backbone-in-global-surveillance-program.

Inkster, Nigel. 2014. “The Snowden Revelations: Myths and Misapprehensions.” *Survival* 56 (1): 51–60. https://doi.org/10.1080/00396338.2014.882151.

Katzenstein, Peter J. 1996. “Introduction: Alternative Perspectives on National Security.” In *The Culture of National Security: Norms and Identity in World Politics*, edited by Peter J. Katzenstein, 1–32. Columbia University Press. https://books.google.nl/books?id=bPjkBhKWBOsC&dq=the culture of national security norms and identity in world politics&hl=nl&source=gbs_book_other_versions.

Kavalski, Emilian. 2013. “The Struggle for Recognition of Normative Powers: Normative Power Europe and Normative Power China in Context.” *Cooperation and Conflict* 48 (2): 247–267. https://doi.org/10.1177/0010836713485386.

Keck, Margaret E., and Kathryn Sikkink. 1998. *Activists beyond Borders: Advocacy Networks in International Politics*. Cornell University Press.

Kittichaisaree, Kriangsak. 2017. “Cyber Espionage.” In *Public Internatinal Law of Cyberspace*, 233–62. Springer.

Libicki, Martin. 2017. “The Coming of Cyber Espionage Norms.” In *2017 9th International Conference on Cyber Conflict (CyCon)*, 1–17. Tallinn: IEEE.

Löffelmann, Markus. 2015. “Regelung Der Routineaufklärung.” *Recht + Politik* 6.

MacAskill, Ewen, Julian Borger, Nick Hopkins, Nick Davies, and James Ball. 2013. “GCHQ Taps Fibre-Optic Cables for Secret Access to World’s Communications.” *The Guardian*, June 21, 2013. https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

Manners, Ian. 2002. "Normative Power Europe: A Contradiction in Terms?" *JCMS: Journal of Common Market Studies* 40 (2): 235–258. https://doi.org/10.1111/1468-5965.00353.

NewsWire. 2018. "Germany's Highest Court Reviewing Country's Permissive New Surveillance Laws." *Homeland Security News Wire*, 2018. http://www.homelandsecuritynewswire.com/dr20180130-germany-s-highest-court-reviewing-country-s-permissive-new-surveillance-laws.

Obermaier, Frederik, Henrik Moltke, Laura Poitras, and Jan Strozyk. 2014. "Vodafone-Firma Soll Für Spähauftrag Kassiert Haben." *Süddeutsche Zeitung*, November 21, 2014. https://www.sueddeutsche.de/digital/neue-snowden-dokumente-vodafone-firma-soll-fuer-spaehauftrag-kassiert-haben-1.2229546.

Riechmann, Deb. 2018. "Costs of Snowden Leak Still Mounting 5 Years Later." *AP News*, June 4, 2018. https://www.apnews.com/797f390ee28b4bfbb0e1b13cfedf0593.

Scheinin, Martin. 2014. "Letter to the Editor from Former Member of the Human Rights Committee." Just Security. 2014.

Schlanger, Margo. 2015. "Intelligence Legalism and the National Security Agency's Civil Liberties Gap." *Harvard National Security Journal* 6: 112–205.

Schulze, Matthias. 2015. "Patterns of Surveillance Legitimization. The German Discourse on the NSA Scandal." *Surveillance & Society* 13 (2): 197–217. http://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/snowden_patterns.

Shubber, Kadhim. 2013. "A Simple Guide to GCHQ's Internet Surveillance Programme Tempora." *WIRED*, June 2013. https://www.wired.co.uk/article/gchq-tempora-101.

Sullivan, Sean. 2013. "NSA Head: Surveillance Helped Thwart More than 50 Terror Plots." *The Washington Post*, June 18, 2013. https://www.washingtonpost.com/news/post-politics/wp/2013/06/18/nsa-head-surveillance-helped-thwart-more-than-50-terror-attempts/?noredirect=on&utm_term=.a517418b486a.

Sunstein, Cass R. 1996. "Social Norms and Social Roles." *Columbia Law Review* 96 (4): 903–968.

Tréguer, Félix. 2016. "Internet Surveillance in France's Intelligence Act." halshs-01399548.

———. 2017. "Intelligence Reform and the Snowden Paradox: The Case of France." *Media and Communication* 5 (1). https://doi.org/10.17645/mac.v5i1.821.

UK. 2015. "Privacy and Security: A Modern and Transperant Legal Framework." https://www.justsecurity.org/wp-content/uploads/2015/03/UK-ISC-Post-Snowden-Report.pdf.

———. 2016. *Investigatory Powers Act 2016*. www.tsoshop.co.uk.

United Nations. 1999. *Resolution Adopted by the General Assembly, Developments in the Field of Information and Telecommunications in the Context of International Security, A/RES/53/70*. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement.

Wahl-Jorgensen, Karin, Lucy Bennett, and Gregory Taylor. 2017. "The Normalization of Surveillance and the Invisibility of Digital Citizenship: Media Debates After the Snowden Revelations." *International Journal of Communication* 11: 740–762.

Wetzling, Thorsten. 2017. "Germany's Intelligence Reform: More Surveillance, Modest Restrains and Inefficient Controls." Berlin. https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf.

Zupančič, Rok, and Miha Hribernik. 2014. "'Discovering' Normative Power as a State Strategy in the Framework of Security, Foreign, and Defense Policy: The Case of Japan." *Philippine Political Science Journal* 35 (December 2014): 78–97. https://doi.org/10.1080/01154451.2014.903566.

Governing Cyberspace

OPEN ACCESS

The publication of this book is made possible by a grant from the Open Access Fund of the Universiteit Leiden.