Big Tech Hits the Diplomatic Circuit: Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord

Robert Gorwa and Anton Peez

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

Chapter 13

Big Tech Hits the Diplomatic Circuit

Norm Entrepreneurship, Policy Advocacy, and Microsoft's Cybersecurity Tech Accord

Robert Gorwa and Anton Peez

INTRODUCTION: MICROSOFT HITS THE DIPLOMATIC CIRCUIT[1]

The "existing and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century," stated the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE) in its first report, published in 2010. Almost ten years later, it has become clear that the use of networked technologies to conduct espionage, sabotage, and subversion (Rid 2013) is a major feature of contemporary global politics (Kello 2017). How this behavior should be governed at the global level has been a major point of international contention, and efforts to develop "cyber norms" of conduct via established international institutions, bilateral summits, and other conventional forms of diplomacy have failed to resolve many fundamental disagreements between key states such as the United States, Russia, and China (Grigsby 2017; Segal 2017; Lantis and Bloomberg 2018; Henriksen 2019). How should the laws of war apply? What kinds of intrusions can be considered an armed attack? What type of networks are fair-play for military cyber commands and intelligence agencies, and what others are off limits?

Unsatisfied with the tenor of the government-led discussion on these issues, Microsoft president Brad Smith proposed a "Digital Geneva Convention" at the RSA Conference in March 2017, calling on states to renounce cyberattacks on the private sector (Smith 2017b, 10). Smith's speech also called upon tech firms to rally together in support of the cause by not collaborating

with governments in cyberattacks, thereby acting as a neutral "Digital Switzerland" (Smith 2017b, 12). In a related initiative from April 2018 onwards, Microsoft has led a coalition of corporations proposing principles of responsible behavior in cyberspace for the private sector.[2] The Cybersecurity Tech Accord, which now has 110 industry members,[3] is a burgeoning industry alliance that appears to be exerting significant influence as a global policy entrepreneur on digital security issues.

In November 2018, the French government presented the "Paris Call for Trust and Security in Cyberspace" (France Diplomatie 2018), an multistakeholder initiative closely planned with Microsoft, but lacking the main cyber powers (Uchill 2018), "teeth" (Matsakis 2018), and ambition compared to the original Digital Geneva Convention proposal (Baker 2018). In this process, Brad Smith has become a global "cybersecurity statesman" of sorts, rubbing shoulders with world leaders, and earning valuable legitimacy as a policy advocate and trusted voice on digital security matters (Gorwa and Peez 2019a, 2019b).

Microsoft's multifaceted initiative—"unapologetically enter[ing] the political sphere" (Jeutner 2019, 170)—warrants a close examination as a novel exertion of corporate influence in international politics. To this end, this chapter will examine the emergence, guiding principles, and participants of Microsoft's various cybersecurity-related initiatives, with a particular focus on the Tech Accord. It will proceed as follows. First, we outline the accord's core normative scope and ambitions, its specific pre- and proscriptions, the involved actors, and norm addressees (Section 2). We then ask and answer three further questions. Why did Microsoft take this step, devoting resources and political capital to an apparent cyber norm-building campaign? Why has Microsoft chosen the "accord" design and employ the language of international humanitarian law throughout its campaign (Section 3)? Finally, why do certain firms choose to sign on to the accord, and who has joined (Sections 4 and 5)?

By answering these questions, this chapter contributes to the recent scholarship on the role of companies in shaping cyber norms (Hurel and Lobato 2020, 2018) in a number of ways. We examine Microsoft's potential motivations for setting up the accord, contextualizing it within the company's 2007–2013 involvement with the U.S. National Security Agency's (NSA) PRISM program and the subsequent PR and consumer trust fallout as one potential reading. Applying literature on international business in global politics, we further identify elements of a "levelling the playing field" strategy and trace Microsoft's actions using an amended "spiral model" of norm entrepreneurship. Next, we explain the accord's design as a nonbinding code of conduct through its flexible and performative benefits, and question the initiative's appropriation of the language of international humanitarian law.

Finally, we present the first descriptive analysis of the Tech Accord's 110 members, and examine the possible instrumental motivations of signatories by collecting and analyzing their public statements regarding accord membership. We argue that most firms—smaller ones, in particular—attempt to cast themselves as innovative "global players" and as impactful technology companies, "bandwagoning" alongside Microsoft.

WHAT IS THE CYBERSECURITY TECH ACCORD?

Microsoft president Brad Smith raised eyebrows in Silicon Valley and beyond when he delivered a keynote at the 2017 RSA security conference that called on states to sign a "Digital Geneva Convention" (DGC), renouncing cyberattacks on the private sector and users, and on companies to not be complicit in such attacks (Smith 2017b). This latter pledge was reformulated as the four-point Cybersecurity Tech Accord and launched in April 2018 by a group of thirty-four technology companies, including not only giants such as Microsoft and Facebook, but also a diverse group of international telecoms, hardware manufacturers, open-source software providers, and cybersecurity threat intelligence companies. The group has since grown in geographic and industry scope to a total of 110 countries, as Microsoft has embarked on a whirlwind global policy advocacy tour.

While Smith's original "Digital Geneva Convention"—certainly the centrepiece of the RSA speech—called for six commitments, the accord features four (see table 13.1). Smith's speech contained elements of what was later launched as the Cybersecurity Tech Accord, then under the heading of a "global tech sector accord" to supplement the DGC proposal (Smith 2017b). While Smith clearly envisioned the DGC to be a company-led process, the main target was still governments. The pledges were formulated as items governments would agree to, with commitments ranging from not "targeting tech companies, private sector, or critical infrastructure" to engaging in "nonproliferation activities [for] cyberweapons." Responding to the feasibility of the DGC in November 2018, Smith described it as a "long-term aspiration" (Smith 2018). The Tech Accord is more modest than the DGC and RSA speech proposal, extending four "core values" to be enacted by companies: no offense, stronger defence, capacity building, and collective action (Tech Accord 2018a). A notable feature is that accord members pledge not only to protect their own customers but also each other's.

Drawing upon Martha Finnemore and Kathryn Sikkink's seminal 1998 article, we define international norms as "standards of appropriate behaviour for actors with a given identity" (Finnemore and Sikkink 1998, 891;

Table 13.1 Commitments and "Common Values" as Proposed by Brad Smith in 2017, and Their Equivalents in the 2018 Tech Accord (Authors' Systematization, Numbers in Parentheses Correspond to the Numbering in the Original Documents)

	Digital Geneva Convention February 2017	*"Global tech sector accord" February 2017 (within the DGC speech)*	*Cybersecurity Tech Accord April 2018*
Addressee →	*States*	*Tech firms*	*Tech firms*
Defense		Collaborative and proactive defense (2); Support for intergovernmental defensive efforts (6)	*Stronger defense:* "Protect all customers globally regardless of the motivation for attacks online"
Capacity building	Assist private sector efforts to detect, contain, respond to, and recover from events (2)		*Capacity building:* "do more to empower developers and the people and businesses that use their technology"
Collaboration	Report vulnerabilities to vendors rather than stockpile, sell or exploit them (3)	Collaborative remediation after attacks (3); Software patches available to all (4); Coordinated disclosure practices for vulnerabilities (5)	*Collective action:* "establish new formal and informal partnerships (. . .) to improve technical collaboration, coordinate vulnerability disclosures, share threats"
Offense	No targeting of tech companies, private sector, or critical infrastructure (1); Exercise restraint in developing cyberweapons (4); Commit to nonproliferation activities to cyberweapons (5); Limit offensive operation to avoid a mass event (6);	No assistance in offensive actions (1)	*No offense:* "companies will not help governments launch cyberattacks against innocent citizens and enterprises"

see also Katzenstein 1996, 5). Early foundational work by Sikkink and Margaret Keck on non-state actors and norms focused primarily on grassroots, transnational advocacy networks (Keck and Sikkink 1998). The authors examined the tactics such networks employ in their attempts to affect

domestic and international policy making. Traditionally, multinational corporations (MNCs) were discussed in the context of the adversarial role they took in relation to these grassroots networks (see also Wolf, Deitelhoff, and Engert 2007). The Tech Accord provides an interesting example of a reversal of this process, with MNCs engaging in their own transnational advocacy and norm-building, which—save for the Paris Call—has been largely separate from civil society and other non-state actors. As Hurel and Lobato (2020) have fruitfully explored for the Tech Accord case, a critical addition to this literature covers corporate entities as norm entrepreneurs (Wolf, Deitelhoff, and Engert 2007; Deitelhoff and Wolf 2013; see also Flohr et al. 2010).

Each accord principle consists of a brief one- or two-sentence explanation, but it is clear that the accord is aimed at companies, rather than at governments. Two of the four principles are relatively uncontroversial: *Collective action* calls for companies to "build on existing relationships and together establish new formal and informal partnerships with industry, civil society and security researchers to improve technical collaboration, coordinate vulnerability disclosures, share threats"—a practice which is already characteristic of the cybersecurity industry and is commonplace among certain vendors and firms (de Fuentes et al. 2017). *Capacity building* is even vaguer, and "may include joint work on new security practices and new features the companies can deploy in their individual products and services" alongside a pledge to help businesses protect themselves from digital threats (of course, many of the companies sell products marketed for this exact purpose). The two more compelling points are those which are more directly related to the original Digital Geneva Convention subject matter of cyberattacks: *no offense* and *stronger defence*.

According to *no offense*, accord signees "will not help governments launch cyberattacks against innocent citizens and enterprises, and will protect against tampering or exploitation of their products and services through every stage of technology development, design and distribution." One major story from the Snowden disclosures described how the U.S. National Security Agency was intercepting routers and other network infrastructure made by Cisco (a signee) mid-transit, reprogramming their firmware to record network traffic and report it back to NSA, and then repackaging them into their original boxes and sending them off to their final international destination (Schneier 2015). In this context, this point could be seen as a pushback against the U.S. national security apparatus, although it is unclear whether companies such as Cisco were aware of this practice (the business maintained it was not). But the language notably does not mention that these companies cannot help states engage in cyberattacks against other states (only against "innocent citizens and enterprises").

Stronger defence involves a commitment to "protect all customers globally regardless of the motivation for attacks online." It allows one to imagine an interesting hypothetical scenario where a cloud provider (such as Microsoft), based in the United States, has to protect servers rented by customers in a country that is a current U.S. adversary from an intrusion effort orchestrated by the NSA or another "Five Eyes" agency. It is exactly this scenario, in which the technology company would be caught between its interests in serving foreign customers as a global business and the national security or espionage-related interests of domestic intelligence agencies that seemed to underlie Smith's original desire to become a "neutral Digital Switzerland." Post-Snowden, it is no longer acceptable for technology companies to be seen publicly as working with intelligence agencies to provide behind-the-scenes access to data. The framing of the accord around "cyberattacks" seems to elide the reality that many of the same effects can be achieved completely legally via government access requests (via for instance, the U.S. Foreign Intelligence Surveillance Court, or FISA court), and in many cases, technology companies that host third-party user data comply with these requests. While an acknowledgment of these government access requests is missing from the Tech Accord, it is discussed by some of the 110 companies that signed on, 40 of whom published their own blog posts or statements discussing the accord and their reasons for joining (tables 13.2 and 13.4). The cybersecurity company Avast, for instance, noted that the accord was particularly important "at a time when world governments are frequently pushing hard for access to user data" (Avast 2018).

Table 13.2 Cybersecurity Tech Accord Members by Industry Sector and by Whether a Press Release Was Issued (as of July 25, 2019)

		Tech Accord members		*Press releases*	
Sector	*Examples*	*Count*	*Share of Tech Accord members (N=110)*	*Count*	*Share within sector*
Information security	FireEye, RSA	38	36%	19	50%
IT	Aliter, Cognizant	20	19%	7	35%
Software	Microsoft, Intuit	17	16%	4	24%
Cloud	Cloudflare, Oracle	8	8%	2	25%
Telecom	KPN, Orange	8	8%	2	25%
Hardware	Dell, HP	6	6%	2	33%
Platform	Facebook, GitHub	5	5%	2	40%
Misc.	WIPFLI, Nielsen	5	5%	2	40%
Industrial	Rockwell, Hitachi	3	3%	0	0%
Sum		**110**		**40**	**36%**

WHY DID MICROSOFT START THE ACCORD?

Why, of all companies, is Microsoft devoting substantial financial and political resources to the development of cyber norms? The Tech Accord has drawn significant media coverage, but little critical analysis to date. Recently, Hurel and Lobato argued that the efforts demonstrate an "an attempt to influence global public policies on cybersecurity" (Hurel and Lobato 2018, 61), and fruitfully applied the IR framework of corporate norm entrepreneurship to the Microsoft case (Hurel and Lobato 2020). Analyses of the Tech Accord have been primarily grounded in the international cybersecurity norms literature, which covers the narrow field of cyber conflict (e.g., Finnemore and Hollis 2016; Grigsby 2017), the broader field of Internet governance and architecture (e.g., Mueller 2010; DeNardis 2014), as well as the intermediary space of cybersecurity. This section applies further IR corporate norm entrepreneurship literature to the case of the Tech Accord, showing that Microsoft is indeed a paradigmatic case for such efforts.

We argue that past work on the Tech Accord has failed to account for Microsoft's recent past and possible readings thereof, and present one such reading. In 2007, ten years before Smith's keynote, Microsoft became the NSA's very first partner in the PRISM program, which involved close collaboration with the government agency to provide clandestine access to sensitive, encrypted user data (*The Guardian* 2013a; Landau 2014, 62–64). In 2013, PRISM came to public attention through the Edward Snowden disclosures. Within a few short years, Microsoft has switched from being engaged in the NSA's surveillance program to aggressively spearheading an initiative to "make the internet a safer place, (. . .) and [retain] the world's trust" (Smith 2017a). We argue that in order to fully understand Microsoft's remarkable current push and role as a corporate norm entrepreneur, this recent history must be considered in detail. The primary factor here is not the actual depth of NSA cooperation, but rather the perceived breach of consumer trust.

Annegret Flohr and colleagues hypothesize that the more vulnerable a company is to a loss of reputation, the more likely it is to engage in norm entrepreneurship initiatives (Flohr et al. 2010, 82). They show empirically that companies with business-to-consumer transactions (rather than business-to-business transactions) are far more likely to engage in norm entrepreneurship (Flohr et al. 2010, 85–94). Over 80 percent of all desktop computers use the Windows operating system (StatCounter 2018), a high rate of interaction with end users. By the firm's own account, two billion people use Microsoft products (Smith 2018). Microsoft representatives address this rationalist explanation by stating that "what is good" for shareholders in this case is also "what is right," by asserting a seamless overlap of Microsoft's business interests and the greater societal good in cyber-norms matters. This, coupled

with the PR fallout from the Snowden revelations, and the waning position of Microsoft as a meaningful corporate player (relative to Google, Facebook, Amazon, and Apple) makes Microsoft a likely candidate for corporate norm entrepreneurship.

Nicole Deitelhoff and Klaus Dieter Wolf make three further particularly relevant points for the case of cyber norm entrepreneurship. First, they argue that corporate involvement in "governance in the post-national constellation" is generally strong (Deitelhoff and Wolf 2013, 222). The realm of cyberspace is emblematic of this setting. Therefore, Deitelhoff and Wolf's work provides a fitting theory to apply to the Microsoft-led case of norm entrepreneurship. Second, the authors amend Risse et al.'s five-phase "spiral model" of state norm socialization (Risse, Ropp, and Sikkink 1999) to fit the corporate context. The adjusted "spiral model" contains the following steps in which businesses deal with human rights norms: (1) denial and "quiet complicity," followed by typically unsuccessful (2) tactical concessions, leading to (3) growing norm acceptance and institutionalization, potentially followed by (4) corporate norm-setting in order to achieve a level-playing field with noncompliant competitors, and finally (5) ongoing rule-consistent behavior, norm-setting and norm development (Deitelhoff and Wolf 2013, 231–234). Third, and more broadly, the authors find that corporate norm entrepreneurship is often primarily driven by "rationalist calculations regarding the re-definition of fundamental business interests" (Deitelhoff and Wolf 2013, 237). In other words, when companies "proactively engage in norm-setting," they are mainly guided by the aim of minimizing losses by bringing competitors who are not adhering to the norm in question into the fold—"levelling the playing field" (Zadek 2004; Deitelhoff and Wolf 2013, 237). This assumption is particularly worth examining in the Microsoft and Tech Accord case.

The remainder of this section proceeds along these three steps. While Hurel and Lobato state that "governments usually look to the ICT industry to prevent, detect, respond to, and recover from cyber attacks" (Hurel and Lobato 2018, 62), governments have also long looked to tech corporations for access to private user data. In the following, we examine this interaction as a key mechanism in understanding Microsoft's ongoing Tech Accord efforts.

A critical element in the call for cyber norms is the difficulty of governing cyberspace in the first place. Cyberspace is today generally considered quasi-regulated space (Jakobi 2013; however, also see Jeutner 2019) and corporate entities are, therefore, crucial actors in this "area of limited statehood," a realm where "the state lacks governance capacities in different sectors or over certain periods" (Börzel and Deitelhoff 2018, 250). Where state governance is limited, corporations are both commonly normatively expected to get involved and empirically more likely to do so (Deitelhoff and Wolf 2013; Börzel and Deitelhoff 2018). The concept of "limited statehood" fits the online context

in many ways—there are few binding rules and governance mechanisms in cyberspace, and the covert nature of cyber activities leads to great difficulties in enforcing any such rules (Kello 2017). The challenges faced by the state-driven and UN-based Group of Governmental Experts (UN GGE, see Grigsby 2017; Henriksen 2019) and the subsequent push by Microsoft and others to establish a loose set of rules for cybersecurity can, therefore, be seen as an attempt to introduce corporate-led norms into the relatively loosely governed area of cyberspace. This presents a difference in both norm entrepreneurs and norm addressees compared to the UN GGE, with corporations acting as both entrepreneurs and addressees. The relatively under-regulated nature of the Internet gives accord signees a—perhaps convincing and reasonable—claim to set cyber policy and standards (Hurel and Lobato 2020, 303–5).

Next, we apply Deitelhoff and Wolf's amended five-step explanatory spiral model for the business context to the case of Microsoft and the Tech Accord. This examination will seek to cover the ten years preceding the presentation of the accord. We argue that Microsoft's cooperation with the NSA on PRISM is a source of the company's norms initiative ten years later. As PRISM's first partner, Microsoft provided the U.S. government with access to U.S. and foreign nationals' data. While the NSA did not have blanket access to user data (as was reported at times, and has been widely misunderstood), the close cooperation between Microsoft and the NSA on FISA orders for foreign nationals' data was nonetheless a major revelation among the Snowden disclosures in July 2013 (*Washington Post* 2013). The fact that the number of Skype calls collected by the NSA tripled after Microsoft acquired the company in 2012 seems to indicate unusually close cooperation between the NSA and Microsoft (*The Guardian* 2013a; Der Spiegel 2013). Once the extent of the PRISM program had been revealed, many companies ardently denied any wrongdoing or responsibility (*New York Times* 2013). Deitelhoff and Wolf identify complicity in government human rights violations as a common point of departure of human rights socialization in the corporate sector. Microsoft's complicity in the broad targeting of foreign nationals' privacy with limited legal process fits this first step.

The second step on the way to norm entrepreneurship are "tactical concessions." Such concessions are driven by the strength of the newfound opposition to the company and its "social and material vulnerability" (Deitelhoff and Wolf 2013, 228, 231). At the time of the Snowden disclosures, the company's marketing campaign stated that "Your privacy is our priority" (*The Guardian* 2013a; Der Spiegel 2013). The PR fallout was swift, and the vulnerability of a corporation so intimately linked to its users' lives was high in the face of the perceived immense breach of trust. Consequently, many of the implicated firms turned to public norm entrepreneurship strategies. In December 2013, Microsoft, Apple, Google and others published an open letter to President

Barack Obama and the U.S. Congress, containing five "reform principles" to reign in government surveillance. They stated that "the balance in many countries has tipped too far in favor of the state and away from the rights of the individual." Brad Smith, then Microsoft's general counsel, put the responsibility for decreasing user trust squarely on the U.S. government's shoulders: "Governments have put this trust at risk, and governments need to help restore it" (*The Guardian* 2013c). In this way, Microsoft sought to highlight their compliance with civil liberty norms, a "regular instance of tactical concessions" (Deitelhoff and Wolf 2013, 230).

The third step—"norm acceptance and institutionalization"—is difficult to separate from concessions. The open letter was accompanied by an industry-wide push for stronger encryption and peer review of application code (*The Guardian* 2013b, 2013c). More antagonistically, Brad Smith compared government surveillance of its servers to "sophisticated malware or cyber attacks" in December 2013 (*The Guardian* 2013b). Microsoft had now accepted and firmly, publicly committed to higher standards, and to no longer providing broad access to user data. Thereby, the company had moved from long-term NSA cooperation to public support for civil liberties online to sharp public criticism of U.S. government practices (see also Hurel and Lobato 2020).

Fourth, this leads to what Deitelhoff and Wolf call "a curious and unexpected side effect"—the potential transformation of "norm-takers into norm-makers." Rather than using discursive tactics such as shaming, Deitelhoff and Wolf argue that companies often change their own behavior and lead by example, forging "collective self-commitments" (Deitelhoff and Wolf 2013, 231–232). The Digital Geneva Convention, Tech Accord, and Paris Call initiatives in 2017 and 2018 are examples of such commitments, as are the company's "Transparency Centres," the "Defending Democracy Program," and their "Digital Crimes Unit" (see Hurel and Lobato 2020). Through this lens and perhaps somewhat favorably, Microsoft's pushes can be interpreted as a genuine effort to drive and advance cyber norms as part of the "groundswell of private leadership" (Matsakis 2018) in this realm from 2014 onwards. In the absence of effective state-led international agreements and therefore the presence of "unregulated space," tech firms such as Microsoft may feel empowered to be more proactive and take the lead in norm and agenda setting, exemplified by the firm's activities as a "quasi-diplomatic actor" (Hurel and Lobato 2018) adopting the vocabulary of international relations.

Fifth, looking into the future, "companies often struggle to commit public actors (. . .) to comply with human rights," particularly in settings of "limited statehood more generally" (Deitelhoff and Wolf 2013, 235). This does not bode well for common cybersecurity norms, and may indeed be the reason why Microsoft toned down the "Digital Geneva Convention" language in the first place (see Smith 2018). The voluntary nature of the accord makes it

increasingly open to interpretation and selective application, raising the question of whether there is any sort of perceived accountability for adhering to its principles at all (Deitelhoff and Wolf 2013, 238). Hurel and Lobato point out that these formal initiatives are only "the tip of the iceberg" (Hurel and Lobato 2020, 292), with Microsoft's norm-making also taking hold through its technical services and policy development, not only explicit public advocacy.

Finally, Deitelhoff and Wolf's observation of attempts to "level the playing field" are particularly apt for the Tech Accord. As this section has illustrated, Microsoft was prominently exposed as an early NSA collaborator in the wake of the Snowden revelations. Following this logic, as a particularly exposed global company (see above), Microsoft had little choice but to go on the offensive and enter the fray as a norm entrepreneur by "mak[ing] the case (. . .) to retain the world's trust" (Smith 2017a, 13)—though not explicitly in connection to the Snowden affair. Microsoft has attempted to do this through adhering to a self-written code of conduct, the Cybersecurity Tech Accord. This code comes alongside a somewhat more skeptical approach to cooperation with governments post-Snowden. Following the commercial necessity of minimizing losses, Microsoft has since attempted to bring tech sector competitors into the fold of also adhering to these higher standards of user protection. As an industry leader, Microsoft is well poised for such a push. This amounts to "levelling the playing field"—that is, bringing competitors up to Microsoft's voluntary standards regarding both governmental cooperation and general cyberattack prevention. Smith himself has chosen his words similarly, describing the Tech Accord in part as an attempt to "create a floor" to prevent a "race to the bottom" (Smith 2018) regarding offensive cooperation with states in cyber affairs.

In conclusion, owing to its early norm entrepreneurship efforts and the absence of major players from the accord (see Section 4), Microsoft has effectively assumed the role as a key spokesperson for tech firms in the cyber-norms debate, thereby creating part of the present-day cyber-norms environment. This, we argue, goes beyond merely carving out a place for themselves within the cybersecurity landscape (Hurel and Lobato 2020). Microsoft has not only aimed for a seat *at* the table, but for the seat at the *head* of the table as the cyber-norms effort grows with initiatives such as the Paris Call.

WHY ARE OTHERS JOINING THE ACCORD?

This section critically analyses the Cybersecurity Tech Accord itself, focusing on the benefits to corporate actors of (1) appropriating of the authoritative language of international humanitarian law without any of its commitment,

and (2) a broad, nonbinding code of conduct open to PR "spin" on behalf of the signatories.

Smith's 2017 Digital Geneva Convention launch was part public relations pitch ("last year we added Advanced Threat Protection for Microsoft Exchange Online") and part plea ("those of us in the tech sector need to act collectively to better protect the internet and customers everywhere from nation-state attacks"). The heavy reliance on international humanitarian law analogies was a guiding theme throughout the original Digital Geneva Convention speech in particular (Smith 2017b). Smith seemed to be directly equating private, profit-maximizing technology firms with humanitarian organizations such as the Red Cross, arguing that just "as the Fourth Geneva Convention relies on the Red Cross to help protect civilians in wartime, protection against nation-state cyber attacks requires the active assistance of the tech sector" (Smith 2017b). Smith's 2017 proposal was critiqued for its sloppy use of the Geneva Convention metaphor: While perhaps a useful mental image, casting oneself in a similar mold as the International Committee of the Red Cross (ICRC), a three-time recipient of the Nobel Peace Prize, offers clear reputational benefits (see also Jeutner 2019, 168). The subsequent 2018 Tech Accord announcement backed away slightly from the Switzerland-related metaphors, as has the branding of the accord. Nonetheless, Microsoft continues to use the semantics of international politics in its broader policy initiatives (Hurel and Lobato 2018, 68), for example, through its "Digital Diplomacy" team (formerly "Global Security Strategy and Diplomacy").

Although consistently discussed as a matter of cyber norms, with norms generally defined as "shared understandings" (for a review, see Niemann and Schillinger 2017), the tenets of the accord seem to be neither particularly shared nor well-understood among the signatories. Given that the public-facing accord is short on detail (comprised of only four points and eight sentences total), it is unsurprising that company statements have varied significantly in how they interpreted the nature and purpose of the Tech Accord. A number of companies stated that they viewed the Tech Accord as an effort to "fight cybercrime" (ESET 2018; Gigamon 2018). Others viewed it as an "alliance" (Avast 2018), with some even invoking it as a tech-company equivalent of NATO's Article 5 collective defence provision (KoolSpan 2018). The accord's August 2018 endorsement of the "Mutually Agreed Norms for Routing Security," an initiative launched in 2014 by the Internet Society (ISOC), shows that the Tech Accord indeed does not only seem to be a set "Accord" but also a loose consortium or alliance that will continue to be involved in evolving Internet governance and technology initiatives.

Unlike the Global Network Initiative (GNI) for preventing censorship and protecting privacy online, or past efforts to bring together technology companies with an overarching human rights goal, there are no publicly

accessible governance mechanisms or accountability frameworks which govern the accord (perhaps because this initiative does not feature any civil society or nonindustry stakeholders). Transparency is summarized in a single line, promising that "we will also report publicly on our progress in achieving these goals"—a far cry from the comprehensive GNI governance charter which details the GNI legal structure and board, along with the detailed requirements for the independent-third party assessments that are undertaken every two years to ensure compliance with the GNI principles (Global Network Initiative 2017). Because the accord is nonbinding, and does not have any clear governance mechanisms, it seems as if it can be, to modify Alexander Wendt's famous formulation, 'what companies make of it' (Wendt 1992).

WHO HAS JOINED THE ACCORD?

To further analyze the Tech Accord's membership, we compiled a list of all members by industry sector,[4] primary world region, date of joining, and whether they issued a press release upon joining.[5] In order to better assess why firms would opt to join the accord, we examined their public justification for doing so, compiling all public statements released by its members. The available blog posts, statements, and press releases were downloaded and assessed for major themes.

The list of signatories is diverse. It includes major platform companies (Facebook, LinkedIn), international telecoms (BT, Telefonica), cybersecurity threat intelligence companies (FireEye, F-Secure, TrendMicro), and PC manufacturers (Dell, Hewlett Packard). Other members include the online payments company Stripe, an enterprise technology company specializing in Tax software (Intuit), and the market research firm Nielsen. By July 2019, a total of 110 companies had pledged to "protect and empower civilians online and to improve the security, stability and resilience of cyberspace" (Tech Accord 2018a).

The tabulation of member statements by line of business and whether they issued a press release (table 13.2) shows that information security firms are most likely to have issued press releases regarding their joining the other firms. Fifty percent of all companies coded as information security firms have issued statements, compared to 29 percent of all remaining firms.

Examining the stated reasons for joining, it is immediately apparent that companies take advantage of the accord to "bandwagon"—proclaiming themselves as innovative, champions of security, and as impactful technology companies alongside Microsoft. This trend was most clear for smaller and less influential firms, eager to name themselves as part of a select group

of globally recognized organizations (emphases added throughout). For instance, Avast, a Czech provider of antivirus software, "joined Microsoft, Facebook, Cisco, and thirty *other tech giants* in what is being considered a 'Digital Geneva Convention'" (Avast 2018); Spanish telecommunications provider Telefónica could brand itself "*among leading* tech companies which pledge to fight cyberattacks" (Telefónica 2018); the Romanian antivirus vendor Bitdefender could announce having joined the accord with "30 *other important players* who have shaped technology throughout the years" (Bitdefender 2018); and the Japanese threat intelligence company Trend Micro suggested that the accord "demonstrates a commitment by *key industry players like us*" (Trend Micro 2018).

Furthermore, the Tech Accord—steered by Microsoft—seems to have pursued a regional strategy of expansion in late 2018 and early 2019 (table 13.3). The two initial waves of membership primarily included firms from the United States and Western Europe. In September 2018, eight Eastern European firms signed on, followed by the first firms from the South America (Argentina and Chile) in November 2018 and January 2019. This finding could be a starting point for research on "how the company develops relations with Global South countries," broadly conceived (Hurel and Lobato 2020, 306; see also Tech Accord 2018b). Since March 2019, new members have once again mainly been from the United States and Western Europe. The complete absence of firms from states such as China, Russia, and Israel indicates that beyond norms for guiding corporate activity in the cyber realm, norms regarding public-private partnership and the relation of the state to its citizens are at stake.

Finally, combining the regional and publicity perspectives, European tech firms seem to be far more keen than their U.S. counterparts to publicly align themselves with the Tech Accord, Microsoft, and cybersecurity advocacy more broadly (table 13.4). While 62 percent of European members issued press releases, only 24 percent of U.S. firms did. This may be because the Microsoft brand might have greater currency in Europe than in the United States, or due to greater anticipated benefits of aligning oneself with user data protection in Europe compared to the United States.

Other than Microsoft, the leading organizer, none of the largest and potentially most impactful members—Facebook, Oracle, and Cisco—released a statement. The role of these major firms within the accord needs to be explored in further research, along with key unanswered questions about the lack of certain major firms that seemingly refused to join (most notably, Google). If the proscriptions of the accord are so flexible, *why not join*? Meanwhile, in the absence of other major players, Microsoft now appears to have taken up the role of spokesperson for the tech industry in this cyber-norms process.

The accord is both performative and flexible, allowing smaller firms to label themselves as meaningful changemakers and innovators, while also potentially allowing larger firms to point to the accord as a token of their goodwill without any meaningful commitments or enforcement mechanisms. If the goal of the Tech Accord is assembling a broad coalition of companies, it is worth pointing out that such flexibility certainly has advantages: It lowers the barriers for entry, perhaps setting the stage for an increasingly rigid process to come (for a policy maker perspective, see Lété and Chase 2018).

CONCLUSION: NEITHER SHARED NOR UNDERSTOOD?

With this chapter, we have sought to trace the evolution of Microsoft's norm entrepreneurship from 2013 Snowden revelations to the 2017 Digital Geneva Convention speech to the 2018 Cybersecurity Tech Accord initiative. We have explored the potential motives shaping Microsoft's behavior as the creator of the accord, unpacked the proscriptions of the accord itself, analyzed public statements issued by signatories to better understand why so many firms have joined, and tabulated its members along various characteristics. At 110 members, it is steadily growing and provides insightful precedent as an informal, potentially powerful coalition of non-state actors in the cyber-norms debate.

We show that Deitelhoff and Wolf's rationalist argument for why corporations may become norm entrepreneurs seems plausible for the Tech Accord and Microsoft case (Deitelhoff and Wolf 2013, 237). The accord may be an attempt to bolster user trust in the companies' data protection measures, a value that has been at the forefront of user demands since 2013. So will this lead to a catalogue of do's and don'ts, a cohesive alternative vision for responsible behavior in cyberspace? Under the commonly accepted definition of norms as "shared understandings" (see Niemann and Schillinger 2017), the accord's provisions and very organizational nature seem neither shared nor understood. Despite the apparent novelty of the initiative, and its ongoing endorsement by scholars frustrated with the current poor state of cybersecurity norms discourse (see, e.g., Tworek 2017; Korzak and Lin 2018), as it stands, the accord offers all the PR potential and heavyweight legitimacy and very little of the normative obligation of the international legal language Microsoft has emulated.

Nonetheless, the rationalist and instrumental accounts do not fully explain the accord, and the goal of profit maximizing "does not rule out the existence of underlying notions of appropriate business behaviour" (Deitelhoff

Table 13.3 Cybersecurity Tech Accord Membership by Date of Joining and by World Region (as of July 25, 2019)

	Wave 1 04/2018	*Wave 2 06/2018*	*Wave 3 09/2018*	*Wave 4 11/2018*	*Wave 5 01/2019*	*Wave 6 03/2019*	*Wave 7 05/2019*	*Wave 8 07/2019*	*Sum*	*Share*
US	21	7	4	5	1	8	14	3	63	57%
Western Europe	8	3	3	2	5	1	1	1	24	22%
Eastern Europe	2	1	8		3	1			15	14%
Asia	1		2			1			4	4%
South America				2	2				4	4%
Sum	**32**	**11**	**17**	**9**	**11**	**11**	**15**	**4**	**110**	

Table 13.4 Cybersecurity Tech Accord by World Region and by Whether a Press Release Was Issued (as of July 25, 2019)

	Tech Accord members	*Issued a press release*	*Share*
US	63	15	24%
Western Europe	24	15	63%
Eastern Europe	15	9	60%
Asia	4	1	25%
South America	4	0	0%
Sum	**110**	**40**	**36%**

and Wolf 2013, 237). Less than half of the accord's signees have issued statements on their joining (tables 13.2 and 13.4), and the biggest, most important members (Facebook, Cisco, LinkedIn, Hewlett Packard, Dell, and others) have been oddly silent regarding the accord, casting some doubt on the assumption of the accord as purely a PR exercise. If all firms are simply seeking to improve their public image through participation, why would they not issue a statement? The importance of individuals such as Brad Smith in driving change may come into play here and is worth exploring further—good-faith commitment to the principles of user privacy and data protection has been traced back to the idealism, ideology, and the institutional culture of the American technology industry (see, e.g., Turner 2008). Another major, unexplored question is why certain major industry players (such as Google) are missing, seemingly having refused to sign on to the accord.

Overall, the Tech Accord demonstrates several novel characteristics which provide a major departure from past norm-building efforts in the cyber realm. It is led by different stakeholders (i.e., tech companies rather than states), and seems to have virtually no external buy-in from civil society, nongovernmental organizations, or other key actors in international cyber governance. However, it seems to be positioning Microsoft as a responsible cyber actor, offering legitimacy for future endeavors, such as the November 2018 Paris Call, which does feature broader civil society participation. Microsoft's tactics can also be interpreted as an attempt to frame the company as a "quasi-diplomatic entity" (Hurel and Lobato 2018, 71), from their spearheading of the Tech Accord to the branding of a "Global Security Strategy and Diplomacy Team," and a way to exercise political influence in a potentially novel way. Watching how this process unfolds will be important for cybersecurity and international norms scholars, and those studying the role of technology and technology companies in politics more broadly.

Notwithstanding the general pessimism and in the cyber community regarding the future of common cyber norms, international norms often start as informal, loose standards and progress to more firm rules—both legally and socially.

NOTES

1. We thank Nicole Deitelhoff, Florian Egloff, Xenija Grusha, and the PRIF PhD colloquium for their helpful comments and suggestions. A previous version of this paper was presented at the inaugural the Hague Program for Cyber Norms Conference, November 5–7, 2018. Many thanks to Dennis Broeders, Corianne Oosterbaan, and the rest of the Hague Program's team for putting this collection together, and for their assistance in turning our initial paper into this book chapter.

2. Industrial manufacturer Siemens has initiated a cybersecurity "Charter of Trust," though with fewer members—16—and less public fanfare (as of July 25, 2019).

3. As of July 25, 2019, the Tech Accord website lists 111 members. Two companies originally announced as joining are now no longer listed, CA Technologies and Symantec (both joined in April 2018). One company currently listed was never announced in a press release, Sharp. For consistency, all three have been omitted from the data used in this paper, resulting in a final list of 110 members.

4. We assign one sector per company, opting for the most significant sector if a company is involved in multiple lines of business. For example, the Japanese conglomerate Hitachi is coded as "Industrial," though it also produces consumer electronics, and Microsoft is coded as "Software" while also offering cloud services. Sectors are defined as follows.

IT: general IT services, web/app development, call centers

Information security: vendors, threat intelligence, security solutions and software (e.g. antivirus)

Telecom: telecommunications firms, internet service providers

Platform: platform companies, social media, online marketplaces

Industrial: heavy machinery, industrial equipment

Software: content management software, tax software, operating systems, apps

Hardware: personal computers, routers, networking and computing hardware

Cloud: web hosting, data storage, cloud services

Misc.: residual category

5. Press releases were searched via online queries for *"Tech Accord" + [company name]*. We assume that there are no language or translation problems with this approach, as the query is not specific to the English language.

BIBLIOGRAPHY

Avast. 2018. "US & UK Issue Security Warning and Tech Giants Join Forces." April 20. https://blog.avast.com/us-uk-issue-security-warning-and-tech-giants-join-forces-avast.

Baker, Stewart. 2018. "If Paris Calls, Should We Hang Up? (11:55 Onwards)." The Cyberlaw Podcast. Episode 240. https://www.lawfareblog.com/cyberlaw-podcast-if-paris-calls-should-we-hang.

Bitdefender. 2018. "Your Protection Is Our Mission, and We're Serious About It." April 17. https://businessinsights.bitdefender.com/your-protection-is-our-mission-and-were-serious-about-it.

Börzel, Tanja, and Nicole Deitelhoff. 2018. "Business." In *The Oxford Handbook of Governance and Limited Statehood*, edited by Thomas Risse, Tanja Börzel, and Anke Draude, 250–271. Oxford, UK: Oxford University Press.

Deitelhoff, Nicole, and Klaus Dieter Wolf. 2013. "Business and Human Rights: How Corporate Norm Violators Become Norm-Entrepreneurs." In *The Persistent Power of Human Rights: From Commitment to Compliance*, edited by Thomas Risse, Stephen C. Ropp, and Kathryn Sikkink, 222–238. Cambridge Studies in International Relations 126. Cambridge, UK: Cambridge University Press.

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

Der Spiegel. 2013. "Wie Microsoft Systematisch Den Geheimdiensten Hilft," July 12. http://www.spiegel.de/netzwelt/netzpolitik/wie-microsoft-mit-fbi-nsa-und-cia-kooperiert-a-910863.html.

ESET. 2018. "ESET Joins Cybersecurity Tech Accord." June 20. https://www.eset.com/int/about/newsroom/press-releases/announcements/eset-joins-cybersecurity-tech-accord-1/.

Finnemore, Martha, and Duncan B. Hollis. 2016. "Constructing Norms for Global Cybersecurity." *American Journal of International Law* 110 (3): 425–479.

Finnemore, Martha, and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change." *International Organization* 52 (4): 887–917.

Flohr, Annegret, Lothar Rieth, Sandra Schwindenhammer, and Klaus Dieter Wolf. 2010. *The Role of Business in Global Governance*. Basingstoke, UK: Palgrave Macmillan.

France Diplomatie. 2018. "Paris Call for Trust and Security in Cyberspace." November 12, 2018. https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf.

Fuentes, José M. de, Lorena González-Manzano, Juan Tapiador, and Pedro Peris-Lopez. 2017. "PRACIS: Privacy-Preserving and Aggregatable Cybersecurity Information Sharing." *Computers & Security* 69: 127–141.

Gigamon. 2018. "Gigamon Joins Cybersecurity Tech Accord." June 20. https://blog.gigamon.com/2018/06/20/gigamon-joins-cybersecurity-tech-accord/.

Global Network Initiative. 2017. "Global Network Initiative Governance Charter." https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/04/GNI-Governance-Charter.pdf.

Gorwa, Robert, and Anton Peez. 2019a. "Charmeoffensiven. Ist Das Schon Außenpolitik, Was Die Großen Technologiekonzerne Betreiben?" *Internationale Politik* 74 (4): 25–29.

Gorwa, Robert, and Anton Peez. 2019b. "Big Tech Hits the Diplomatic Circuit." Berlin Policy Journal/German Council on Foreign Relations (DGAP)). https://berlinpolicyjournal.com/big-tech-hits-the-diplomatic-circuit/.

Grigsby, Alex. 2017. "The End of Cyber Norms." *Survival* 59 (6): 109–122. doi:10.1080/00396338.2017.1399730.

Henriksen, Anders. 2019. "The End of the Road for the UN GGE Process: The Future Regulation of Cyberspace." *Journal of Cybersecurity* 5 (1). doi:10.1093/cybsec/tyy009.

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

Hurel, Louise Marie, and Luisa Cruz Lobato. 2018. "Unpacking Cyber Norms: Private Companies as Norm Entrepreneurs." *Journal of Cyber Policy* 3 (1): 61–76.

Jakobi, Anja P. 2013. "Non-State Actors All Around: The Governance of Cybercrime." In *The Transnational Governance of Violence and Crime*, edited by Anja P. Jakobi and Klaus Dieter Wolf, 129–148. London, UK: Palgrave Macmillan. doi:10.1057/9781137334428.

Jeutner, Valentin. 2019. "The Digital Geneva Convention. A Critical Appraisal of Microsoft's Proposal." *Journal of International Humanitarian Legal Studies* 10 (1): 158–170. doi:10.1163/18781527-01001009.

Katzenstein, Peter J. 1996. *The Culture of National Security: Norms and Identity in World Politics*. Columbia University Press.

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

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven, CT: Yale University Press.

KoolSpan. 2018. "An Enduring Principle: KoolSpan Joins Cybersecurity Tech Accord To Lead Industry Efforts For Collective Cyber-Defense." https://koolspan.com/koolspan-joins-cybersecurity-tech-accord/.

Korzak, Elaine, and Herb Lin. 2018. "Proposal for a Cyber-International Committee of the Red Cross." *Lawfare*. October 17. https://www.lawfareblog.com/proposal-cyber-international-committee-red-cross.

Landau, Susan. 2014. "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations." *IEEE Security & Privacy* 12 (1): 62–64.

Lantis, Jeffrey S., and Daniel J. Bloomberg. 2018. "Changing the Code? Norm Contestation and US Antipreneurism in Cyberspace." *International Relations* 32 (2): 149–172.

Lété, Bruno, and Peter Chase. 2018. "Shaping Responsible Behavior in Cyberspace. Workshop Briefing Paper." The German Marshall Fund of the United States. http://www.gmfus.org/publications/shaping-responsible-state-behavior-cyberspace#.

Matsakis, Louise. 2018. "The US Sits Out an International Cybersecurity Agreement." *Wired*, November 12. https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/.

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance*. Information Revolution and Global Politics. Cambridge, MA: MIT Press.

New York Times. 2013. "Report Indicates More Extensive Cooperation by Microsoft on Surveillance," July 11. https://www.nytimes.com/2013/07/12/us/report-indicates-more-extensive-cooperation-by-microsoft-on-surveillance.html.

Niemann, Holger, and Henrik Schillinger. 2017. "Contestation 'All the Way down'? The Grammar of Contestation in Norm Research." *Review of International Studies* 43 (01): 29–49. doi:10.1017/S0260210516000188.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. London: Hurst & Company.

Risse, Thomas, Stephen C. Ropp, and Kathryn Sikkink, eds. 1999. *The Power of Human Rights: International Norms and Domestic Change*. Cambridge, UK: Cambridge University Press. http://ebooks.cambridge.org/ref/id/CBO9780511598777.

Schneier, Bruce. 2015. "Cisco Shipping Equipment to Fake Addresses to Foil NSA Interception." March 20. https://www.schneier.com/blog/archives/2015/03/cisco_shipping_.html.

Segal, Adam. 2017. "The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What?" *Council on Foreign Relations*. June 29. www.cfr.org/blog/development-cyber-norms-united-nations-ends-deadlock-now-what.

Smith, Brad. 2017a. "The Need for a Digital Geneva Convention. Blog Post." *Microsoft on the Issues*. February 14. https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

———. 2017b. "The Need for a Digital Geneva Convention. Transcript of Keynote Address at the RSA Conference 2017." https://blogs.microsoft.com/uploads/2017/03/Transcript-of-Brad-Smiths-Keynote-Address-at-the-RSA-Conference-2017.pdf.

———. 2018. "Digital Peace in an Age of Cyber Threats. Speech and Q&A at the Peace Palace, The Hague, the Netherlands." November 6, 2018.

StatCounter. 2018. "Desktop Operating System Market Share Worldwide. September 2017–September 2018." http://gs.statcounter.com/os-market-share/desktop/worldwide.

Tech Accord. 2018a. "Cybersecurity Tech Accord. Protecting Users and Customers Everywhere." https://cybertechaccord.org/accord/.

———. 2018b. "Cybersecurity Tech Accord Expands Rapidly; Announces Partnership with Global Forum on Cyber Expertise (GFCE)." https://cybertechaccord.org/gfce_partnership/.

Telefónica. 2018. "Telefónica among Leading Tech Companies Which Pledge to Fight Cyberattacks." April 17. https://www.telefonica.com/es/web/public-policy/blog/articulo/-/blogs/telefonica-amongst-leading-tech-companies-which-pledge-to-fight-cyberattacks.

The Guardian. 2013a. "Microsoft Handed the NSA Access to Encrypted Messages." July 12. https://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

———. 2013b. "Microsoft Likens Government Snooping to Cyber Attacks." December 5. https://www.theguardian.com/technology/2013/dec/05/microsoft-likens-government-snooping-cyber-attacks.

———. 2013c. "Twitter, Facebook and More Demand Sweeping Changes to US Surveillance." December 9. https://www.theguardian.com/world/2013/dec/09/nsa-surveillance-tech-companies-demand-sweeping-changes-to-us-laws.

Trend Micro. 2018. "The Cybersecurity Tech Accord: Time to Come Together to Combat Digital Threats." April 17. https://blog.trendmicro.com/the-cybersecurity-tech-accord-time-to-come-together-to-combat-digital-threats/.

Turner, Fred. 2008. *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, IL: University of Chicago Press.

Tworek, Heidi. 2017. "Microsoft Is Right: We Need a Digital Geneva Convention." *Wired*, September 5. https://www.wired.com/2017/05/microsoft-right-need-digital-geneva-convention/.

Uchill, Joe. 2018. "U.S. Hasn't Signed Cyber Principles—yet. 13 November 2018." *Axios Codebook*. November 13. https://www.axios.com/newsletters/axios-codebook-66eb6017-f7ff-4f10-a0b5-1018a441cc43.html.

Washington Post. 2013. "Here's Everything We Know about PRISM to Date." June 12. https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

Wendt, Alexander. 1992. "Anarchy Is What States Make of It: The Social Construction of Power Politics." *International Organization* 46 (2): 391–425.

Wolf, Klaus Dieter, Nicole Deitelhoff, and Stefan Engert. 2007. "Corporate Security Responsibility: Towards a Conceptual Framework for a Comparative Research Agenda." *Cooperation and Conflict* 42 (3): 294–320. doi:10.1177/0010836707079934.

Zadek, Simon. 2004. "The Path to Corporate Responsibility." *Harvard Business Review* 82 (12): 125–132, 150.

Governing Cyberspace

OPEN ACCESS

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