Cyber-Norms Entrepreneurship? Understanding Microsoft's Advocacy on Cybersecurity

Louise Marie Hurel and Luisa Cruz Lobato

Chapter 14

Cyber-Norms Entrepreneurship?

Understanding Microsoft's Advocacy on Cybersecurity[1]

Louise Marie Hurel and Luisa Cruz Lobato

> In 2016, a mantra, "There's no national security without cybersecurity," took hold within Microsoft and started to seep into the public discussion. We were hardly alone with this recognition. As German conglomerate Siemens AG predicted succinctly, "Cybersecurity is going to be the most important security issue of the future." Clearly, any issue that would be fundamental to national security would propel the tech sector even more squarely into the world of international diplomacy. (Smith and Browne 2019, 110)

In February 2017, Microsoft called for the establishment of a Digital Geneva Convention, as a direct response to the expansion of state-sponsored cyberattacks. According to the company's president, Brad Smith (2017), such commitment should be of utmost importance for maintaining peace and stability in cyberspace, given that "nation-state hacking has evolved into attacks on civilians in times of peace." It is now common sense that most of the contemporary infrastructure that anchors the Internet is owned by private actors (Abbate 1999; Kitchin 2014; Musiani et al. 2016). This also means that potential targets include datacenters, servers, and devices; that is, the infrastructures owned by Microsoft and its industry peers as well as the data from its customers. While the Digital Geneva Convention was then met with different degrees of enthusiasm and skepticism by diplomats, scholars, and governments alike (Grigsby 2017; Interview, October 2019), as Brad Smith noted, "[a]t least we had succeeded in sparking a new conversation" (2019, 83).

The call for the Geneva Convention is not the first nor the last effort from the private sector to secure their infrastructure against state-sponsored attacks. Other Microsoft initiatives, such as the Tech Accord, the Paris

Call for Trust and Security, the CyberPeace Institute and engagement with governments—bilaterally or via international organizations—(Barrinha and Renard 2018), suggest that, at least, when it comes to cyberspace, companies have devised distinct regulatory and organizational strategies to build their legitimacy to negotiate with states. Of particular interest is the fact that their legitimacy as political actors is once again being debated.[2] What is more: Microsoft's involvement with the cyber norms-making has reanimated much of the talk on norms and private governance, as it becomes evident from the number of recent debates on this topic.[3]

We take the contestation over Microsoft's legitimacy as norm entrepreneur as an entry point to the discussion of how global cybersecurity governance unfolds in practice and how, instead of focusing on either the "public" or "private" aspects of it, cybersecurity governance happens in a grey zone of continuous contestation and negotiations over *who can engage in norms-making, how norms are made* and *what counts as norm*. In a previous study, we paid attention to the first question, looking at how private actors shape cybersecurity by means of public-private partnerships, lobbying, and self-regulation (Hurel and Lobato 2018). Now, we take a step further and look at how organizational complexity might highlight different modalities of exerting influence on public policy and engage in an interdisciplinary effort to portray the socio-technical arrangements (both intra-organizationally and internationally) as parts of a norms-making continuum. This exercise is relevant to the study of power, influence, agency, and authority in global cybersecurity governance, as it allows us to grasp the specific organizational, technical, and material arrangements that support the practices of stakeholders to negotiate their conditions of engagement in cybersecurity governance. Furthermore, these strategies allow us to deepen the critique of *who* produces norms so as to address the ontological problem of *what* it is to *produce* a norm.

In this chapter, we seek to provide two major contributions to the ongoing debate on cyber norms. The first contribution is with respect to how norms are usually conceived within this debate. Rather than being contained in the written text (law and regulation), norms extend to the processes (see Finnemore and Hollis 2016) of negotiation that happen until it reaches its "final" (written) and also to the agencies, resources, and organizational and technological structures that are mobilized in order for it to reach widespread public debate. The "expectations of behavior" that are a necessary component of norms also come in different forms, including through an infrastructure of access established to promote values such as transparency and trust (e.g., Transparency Centers). The second relates to the understanding of how global cybersecurity governance unfolds in practice and which agencies count as legitimate in the process of negotiating cyber norms. As we argue, the question of who's agency should count in cybersecurity norms development is also indissociable from the question of *how* norms-making processes are perceived and conceptualized.

We look specifically at Microsoft as a case composed by a plethora of dimensions, including a somewhat intriguing diplomatic engagement. In spite of its global reach, the company has consistently expanded the legal and policy engagement, developed an extensive list of cyber norms-specific documents, and invested in international cybersecurity initiatives (to name a few), all of which come together with promoting security of their services and products. These and other dynamics have raised important questions as to what kind of role the private sector plays in global cybersecurity governance. Some scholars have referred to these continuous efforts as "tech diplomacy" or "corporate foreign policy" (*Economist* 2019). We argue that such developments have resurfaced (see Hurel and Lobato 2018; Gorwa and Peez 2018) important discussions related to the different modalities of engagement of the tech sector in shaping and taking part in global/international cybersecurity.

We purposefully make use of the term "norms entrepreneurship" to engage with a more critical discussion of what constitutes as norms-making in cybersecurity governance while simultaneously proposing a different starting point to the discussion, that is, the formal and informal practices within the private sector. This task is guided by the questions of *how can we understand the role of private actors in cybersecurity governance* and *what it has to say about norms promotion.* Methodologically, we draw on an analysis of Microsoft's practices that could be traced from qualitative interviews conducted with company's representatives from different parts of the world, the analysis of policy documents published by its Diplomacy Team, information circulated in press releases and media headlines, and participant observation in different international and regional cybersecurity events. In the first section of this chapter, we assess different bodies of literature to conceptualize private governance and question whether there is something unique to be said about Microsoft's engagement in cybersecurity governance. Second, we provide an in-depth discussion on the role of technical mediation and organizational complexity as constitutive elements of corporate agency and norms-entrepreneurship in cybersecurity. Third, we engage with a more theoretical discussion on "how norms become norms," exploring the ways in which Microsoft engages in "diplomatic" practices. With this, we expect to provide a contribution to the existing IR literature on norms and private governance by showing how negotiations over who's a legitimate norm entrepreneur also depend on an overlap or blur in the line dividing the public/private, and to ongoing discussions on cyber norms, by raising the question of what counts as a norm and how norms are built-in practice.

FROM NORM TO NORMATIVE ARRANGEMENTS: PRIVATE GOVERNANCE AS A FRAMEWORK

Norms are fundamental international institutions that both describe and prescribe action in this world (Finnemore and Sikkink 1998; Onuf 1989; Wendt 1992; 1995). As such, norm advocacy is an important formal dimension of international governance in the most distinct spheres of international life—cybersecurity being no exception. It presents a way of compromising states and biding their behavior to particular technical, professional, and political agreements as to which actions to take to avoid, mitigate, and overcome threats and risks in cyberspace. There has been far less attention to this dimension of private governance in cybersecurity scholarship.[4] As we argued elsewhere (Hurel and Lobato 2018), IR literature on norms presents an important first step to approach this gap. But it is not enough, for it offers a far less nuanced perspective on how different kinds of private groups engage with shaping international norms of behavior for state actors.

In this chapter, we look at private governance as a way to emphasize the distinct normative arrangements that might come with corporations taking the stage in norms promotion. This requires us to revisit and question how norms promotion has been conceptualized thus far (sections two and three) so as to encompass a multiplicity of ways in which values are communicated with more established interlocutors in the field of norms-making. What follows is an exercise to first single out the ways in which corporate action has already been conceived in global governance, management, and media and communications studies, followed by a discussion on the relevance of looking at Microsoft as a case that is both *sui generis* when compared to what has been addressed by scholars across different disciplines and *unique* in its own organizational, situational, and contextual dynamics. Cases such as Microsoft call for an approach to cyber norms-making that is able to encompass the modularity, or perhaps, blurriness between its *sui generis/unique* character. Private governance allows us to approach this complex enmeshment between social, technical, material, and discursive arrangements that configure how the company influences and engages in cybersecurity governance.

Private governance is not typically recognized as a dimension of public policy making, despite the indisputable role of private actors in designing formal and informal rules for products, establishing sectoral regulation in tech, certifying professional competency and setting technical standards that impact society at large (Hall and Biersteker 2002; Rudder, Fritschler, and Jung Choi 2016). In cybersecurity, private actors have recognizably played a fundamental role in ensuring operational and technical security, as they help to set standards, determine authentication and trust mechanisms for both infrastructures and services, provide expertise, develop software, hardware, as well as hold considerable knowledge on cybersecurity risks and threats. However, their role in shaping formal and informal rules of behavior in cyberspace remains undertheorized.

Scholars in international relations[5] and management studies have long emphasized the role of private actors in a number of global governance fields (Strange 1998; Gilpin 1976; Avant 2005; Abrahamsen and Williams 2009; Leander 2010). Drawing from the end of the Cold War, many of the early IR literature on private governance focused on the effects of globalization and the need for new mechanisms and perspectives to cope with transnational challenges, jurisdiction, and international flows (Benz et al. 2007). This opened up an avenue for thinking "beyond the state" or what has been referred to as "governance without government" (Rosenau and Czempiel 1992) and a move from "government to governance" (Mayntz 2003). On the one hand, this perspective opens up the possibility for considering the agency and influence of actors other than states. On the other hand, it is important to note that this was also a period where the global market was opening up and with many countries, especially the United States, favoring competition and privatization of the public realm. Fuchs (2007) suggests that these were important enablers to the consolidation of, at least, three dimensions of business as an actor in global governance: instrumental power (lobbying, campaign, and party finance), structural power (capital flows as enablers to agenda-setting power, self-regulation, and PPPs), and discursive power (legitimation and political authority).

Management studies, on the other hand, has explored extensively the role of corporate governance and the development of further mechanisms of behavior, such as Corporate Social Responsibility (Bies et al. 2007; Mason and Simmons 2014). These mechanisms attempt to outline some of the political roles and responsibilities that companies should undertake. Literature on CSR also focuses on "how corporations facing governmental deficits can solve public problems independently or through multistakeholder initiatives to improve social welfare" (Westermann-Behaylo, Rehbein and Fort 2015, 389). This view resonates with a "governance without government" view that is rooted in self-regulation and privatization of different public services. It portrays the private sector as a necessary actor and as an intervenor that will ultimately produce positive outcomes in this exercise of "filling the gaps" *where* and *when* government fails to do so. This view holds the assumption that in a globalized world, business is better positioned to work as global interlocutors—combining the creation of value for their shareholders and for society (see Garriga and Melé 2004).

What is interesting in this particular approach to corporate governance within management studies is that, whereas it rightly points to an increase in private actors' competencies in a number of relevant governance themes, it misses the fact that they do not act only where and when governments fail. The 1980s opening of global markets also enabled an increase in the "spaces" in which companies could act by means of the delegation of a number of state competencies to the private sector (privatization) as well as the incorporation of market rationales into government functions (marketization), a number of new fields of intervention and competition opened to private companies (Bevir 2009; Crouch 2004). However, rather than meaning that corporations would "fill the gap" left by governments, this opening up provided for new spaces for *contested* and *negotiated* governance, that is to say, in which corporations and government actors had to, at all times, negotiate their own roles in it. What is more: with the so-called revolving door between public and private sectors (which was observable also from the professional backgrounds of part of our interviewees at Microsoft), part of the negotiations likely benefit from a shared understanding and grammar about what kinds of approaches and issues should be prioritized in public policy and how. Thus, rather than taking place in the absence of "public" governance, "private" governance is often deeply intertwined with it (Lobato 2016).

In this sense, contemporary private governance presents us with important challenges. First, it is difficult to define the boundaries of private groups' decisions that make it into public policy. Whereas private organizations make policies that affect the larger public, their rule-making functions often remain concealed by a variety of forms they take—which includes trade associations, not-for-profit organizations, and public policy teams within for-profit enterprises. Second, their operations can result in a lack of transparency, accountability, and legitimacy that is required of governments, despite the fact that private groups make and enforce rules that bind people to follow them, just like governments' laws and regulations (Rudder, Fritschler, and Jung Choi 2016).

Notwithstanding these challenges, this is a significant area of cybersecurity governance that deserves further scrutiny. Despite the often tacit recognition of private groups' role in shaping cybersecurity, there is scant empirical analysis on how this happens and through which venues.[6] This might possibly be due to a difficulty in accepting that companies' practices, such as lobbying, and principles-based action, including norms promotion, are not mutually excluding. Companies are very often analyzed under the terms of rational choice theory: they are usually seen as rational actors, acting on a cost-benefit based evaluation, rather than by any "common good" incentives. Claims of companies acting on moral or normative grounds are promptly criticized either because corporations cannot be morally distinguished from the human beings that constitute them (Rönnegard 2015) or because companies, even when acting on social ends, are seen to do so exclusively to maximize profits (Friedman 2007). And when companies are recognized as possibly acting on some kind of normative or social grounds, it is argued that, when doing so, they are not reduced to the actions and interests of their members. The challenge is, therefore, one of continuously attempting to locate agency amid a complex and evolving organizational structure in a context where perhaps that is not possible.

When it comes to cybersecurity, the increasing digitization of society and governments' reliance on informational infrastructures (cloud computing and data centers) provides a significant element to thinking about norms entrepreneurship and private governance, more generally. Business models are in constant development and this includes, but is not restricted to the (i) diversification of services and products, (ii) continuous organizational flexibility (new teams, posts) and (iii) key leadership influence. It plays a fundamental part in understanding the socio-technical dimension of private governance of actors *such as* Microsoft. The development of solutions and services requires careful consideration as it embeds specific protocols and functionalities that are selected to maintain a secure ecosystem. On the one hand, these arrangements prescribe what kind of security is "desirable" and "available" for consumers (public or private) (Hurel 2018) through technical architectures, protocol specifications, and security control mechanisms. Media and Communications scholars have drawn on science, technology and society studies to expose emerging dynamics of power of platforms and infrastructures (Kitchin 2014; Gillespie 2017; Plantin et al. 2017; Gorwa 2019). They consider protocols, algorithms, infrastructures, technical systems as an integral part of the governance *of* and *by* platforms. On the other hand, the development of products and services happens within a wider framework of overarching principles (trust and security), objectives and/or company strategies.

Understanding how corporate actors promote norms in cybersecurity, therefore, requires an integrated perspective between the socio-technical, organizational, and political arrangements. As the following sections show, the visibility of these configurations is indispensable and perhaps indissociable in understanding private influence in cybersecurity governance, in general, and norms-entrepreneurship, in particular. As one of our interviewees suggested, the global and diplomatic engagement is part of a continuum of what is done and advocated for on the enterprise side of the company. Though often-invisible to cyber-norms discussions, these arrangements provide the conditions of existence for the big tech companies to exert influence and maintain their engagement nationally, regionally, and globally with different stakeholder groups.

As this chapter seeks to illustrate, norms-making and entrepreneurship are not restricted to echoing or proposing new terms or international norms; rather, it encompasses a complex negotiation of the values and services and is enabled by continuous organizational flexibility and key leadership influence.

Therefore, delving into the practices of companies and showing how complex structures of governance work offers us a privileged take on how different kinds of norms are produced and negotiated. It also allows us to go deeper into the different practices adopted by the company so as to show that norms may come in a variety of shapes—the Tech Accord and the Digital Geneva Convention are but the tip of the iceberg; contemporary corporate entrepreneurship also comprises voluntary self-commitments in reaction to public expectations, rather than simply being a response to "delegated tasks" (Hurel and Lobato 2018, 67).

Unlike other big tech companies, Microsoft engages as much in platform governance[7]—by embedding compliance within their platform, for example, making sure that it is not being used to violate intellectual property, and so on—as they seek to establish room for themselves as both industry leaders *and* government interlocutors (Interview, September 2019). When asked about why would a company get involved with cyber norm promotion, an interviewee answered that global companies should be able to put governments to talk and that it is impossible for governments to do it all [the governance work in cyberspace] by themselves. At the same time, however, s/ he emphasized that it is of fundamental importance that governments and companies act together in combating cybercrime, for example, and that corporations are unable to pursue this task by themselves (Interview, September 2019). Also part of Microsoft's business strategy (Interview, October 2019), norms become important meaning settlers and indicators of commitment between parties. In addition to engaging in lobbying with national governments, the company has for some time now raised interest for its explicit advocacy on norms of state behavior in cyberspace (Smith 2017). As we will explore in detail in section three, such engagement means that, despite obvious resistance and suspicion on the part of governments (and diplomats the most), the company is effectively *there* (in the meeting room) when it comes to discuss and negotiate action and norms with states.

Several times when conducting this research, we were met with the question of *why* we were looking at Microsoft, or if, due to its open advocacy and engagement with norms promotion, this would not be an exceptional case rather than a pattern, or even whether we could provide any valuable generalization from this case. Particularly interesting about Microsoft's case is that, because it is *sui generis* and not (yet) followed by its peers in the private sector when it comes to openly carving out a space for itself as a legitimate interlocutor in norms debate, it offers us with a yet underexplored perspective on potential new unfoldings of private practices in global governance. While they indeed embrace much of the patterns for private action that are identified by specialized literature—hybridization, revolving door, reliance on PPPs, increased participation in decentralized governance processes, for example, via platform governance, and so on—they also bring to the analysis a unique take on the way in which the organization's complexity—that is, the structures, people, technologies, and processes, that hold them together—makes it into the construction of this particular kind of legitimation that might be very similar and yet quite distinct from traditional corporate lobby, and what is more, substantially affect how we conceive norms. It is the curiosity with the kinds of practices that become part of cybersecurity governance by means of Microsoft's actions that moves us. Thus, rather than the question of why Microsoft is doing this, what interests us the most is the question of *how* they are doing it—and what it means for cybersecurity governance.

CYBER NORMS AND TECHNICAL/ TECHNOLOGICAL MEDIATION

An immediate consequence to the endeavor of singling out Microsoft yields an important question of whether there is something special about the company and how it operates. We argue that yes, there is. Not necessarily because Microsoft is a stand-alone case, but because perhaps the inquiry and study of norms and governance in cybersecurity requires more attention to particular socio-technical, organizational, and political arrangements and their role in shaping cybersecurity. We argue that unique dispositions within Microsoft (e.g., product, change in business model, organizational history and structure and leadership) provide an incrementally dynamic setting for specific modalities of influence, legitimacy-making and norms-setting to emerge. This arrangement includes a combination of practices—discourses, service provision, technical arrangements, knowledge and expertise—that support and configure norms-making and their capacity to engage in norms-entrepreneurship in cybersecurity.

It can be said that Microsoft's efforts to become a legitimate actor in cybersecurity norms-making depend on a double mobilization: the first is the assembling of an organizational structure that provides a seemingly comprehensive narrative not only to the task of engaging with governments (thus, including but not being restricted to government relations departments), but also to its "global" engagement with the topic of norms-making (e.g., Diplomacy Team). Of course, this coherence might be only apparent (e.g., it might be that most of the "diplomatic" work stems from the presidency). However, it matters that "public-facing" structures are able to hold within the broader attempt to fit the company's efforts on a coherent framework of action. This first mobilization has been and will continue to be explored continuously throughout the chapter.

The second mobilization, in turn, corresponds to the expectations over certain kinds of desired (state) behavior that are embedded in both their modes and infrastructures of engagement with governments (e.g., via Transparency Centers, its Digital Crimes Unit) and technological services—including the kinds of shifts in business strategies that have been adopted in the past years. Considering both these dimensions, we now turn to an examination of how technical, technological, and organizational affordances are productive of norms and advance the claim that norms are also embedded in the kinds of technical and technological mediations in place when the company interacts with states.

A Little Bit of Organizational Complexity

Microsoft works to socialize a common understanding of security concerns between tech companies (e.g., Business-to-Business security solutions) and governments—through activities that range from public-private partnerships (PPP) to a more direct engagement in proposing and influencing policy development. In what follows, we highlight three ways in which associations between the technical and organizational initiatives characterize Microsoft's normative influence on cybersecurity.

First, they do so by providing technical expertise and services. As a big tech company, Microsoft has developed a suite of services and products that aim at providing effective protection of infrastructures and data sets, promote the stability, resilience and security of systems, and facilitate logistics and data management. Concerns at the enterprise level seek to address issues related to authentication, trust, identity and access management, interoperability, and incident detection and mitigation. This perspective frames security as a service, as a set of techniques, and as expert knowledge about threats and vulnerabilities.

The provision of security services for governments takes the form of public-private partnerships and is contextualized in a customer-company relation. However, a "business-as-usual" approach to PPP has raised significant amounts of critique related to the expected role of governments as legitimate actors for providing security. Further concerns include the risk of incurring on a market-driven approach to cybersecurity (Carr 2016)—or "privatisation of security" (Avant 2005)—and the abdication of the state in protecting critical infrastructure (see Assaf 2009; Dunn Cavelty and Suter 2009). Notwithstanding, cooperation among both sectors is, as Dunn Cavelty and Suter note, "simply essential" when it comes to securing interconnected systems (2009, 180). On the one hand, PPPs refer to a particular way of outsourcing security services and expertise (also see Berndtsson and Kinsey 2016). On the other hand, this particular kind of expertise-driven engagement presents security as a feature—de-politicized, flattened, and technical in nature. Security is habitualized (see Berger and Luckman 1987) as an unquestioned set of assembled components (e.g., standards, packages, platforms, products) and exported as a ready-made product to governments (see Simos 2018). As McIntyre[8] suggests (2017), "we in the industry can better serve governments [. . .] by incentivizing migrations to newer platforms which offer more built-in security; and that are more securely developed." In a less visible manner, security is shaped through design—for example, through standards for hybrid cloud infrastructure, vulnerability management, security development life cycle, encryption and communication standards.

Technical PPPs are a fundamental form of engagement between Microsoft and local governments. These cooperation mechanisms allow them to socialize particular forms of security management and threat assessment, establish channels for information sharing, and create new avenues for trust-building. That is the case of the Government Security Program, their regional Transparency Centers (United States, Singapore, Belgium, Brazil, and China), and the Digital Crimes Unit (DCU) team, where Microsoft provides tailored security services and responds to cyberattacks—which includes source code sharing, information on malware, threats and vulnerabilities (Microsoft 2014; Government, n.d.). The DCU's Cybercrime Center gathers law enforcement, NGOs, academics, and industry in combating different modalities of crime—cloud crime and malware, misappropriation of Microsoft intellectual property, deterring nation-state actors, and online child exploitation—through networks of collaboration and by using (and promoting) secure technology deployment (e.g., cloud, PhotoDNA) (Digital, n.d.). Moreover, it took down six domains of the Russian hacking group accused of having launched a phishing campaign in the 2016 U.S. presidential election (Newman 2018). Cases such as the GSP and DCU provide a space where governments and industry can closely operate in taking down cybercriminal networks. Most importantly, the close collaboration between law enforcement and Microsoft DCU also relies on the recruitment of investigators and former prosecutors. The "revolving door" between both sectors in cases such as this provides a rather blurry distinction between public and private as the exchange between both (in terms of skills, expertise, and personnel) is a significant factor to coordinating responses.[9]

Second, they engage with policy to establish and/or reinforce specific values. This is not new. In 2005 Microsoft had advocated for a comprehensive privacy legislation in a speech to the Congressional Internet Caucus (see Microsoft 2005). Back then there was little response from the government, and concerns with privacy were only starting to emerge. Even so, the practice of prescribing specific principles for specific legislations on data privacy was the same then as it is now. In light of the diversification of services and products rooted in cloud computing and artificial intelligence, Microsoft's influence is also characterized by constant attempts at flagging new areas for public regulation (e.g., artificial intelligence and facial recognition) and greater corporate social responsibility (Smith 2018).[10] Though these suggestions are partly directed toward the construction of a narrative around common goods or shared values across society, government, and industry, there is an inherent "causal link" that "protecting consumers promotes commerce, and that's good for everyone" (Microsoft 2005). In the case of facial recognition, the company, as a leader in the development and application of such a technology, holds considerable knowledge and expertise over the technical and use-specific requirements—which also serves as leverage on claiming their say on how a technology-specific regulation should look like. Within this framing, it is not unlikely that this engagement with policy comes as a direct action from industry in seeking to influence the principles and legislation that will regulate the very technologies they work with.

Third, they advocate for international cooperation and cybersecurity norms. As previously mentioned, technical expertise and policy engagement at the national level highlight important dimensions of the association between the technical and organizational activities within the company. However, when it comes to international cyber norms, Microsoft faces a greater challenge in communicating the importance of including the private sector in a (originally conceived as) state-centric realm. Back in 2012, the consolidation of international debates on Internet governance was seen as a fruitful starting point for thinking about new PPP models for promoting international cybersecurity norms (see Hurel 2016).[11] As Matt Thomlinson (2012), former VP of Security at Microsoft noted, "global conversations on cybersecurity would also benefit from a private sector perspective that can help governments think through the technical challenges and priorities involved in securing billions of customers using the Internet around the world."

After having taken a proactive measure in advocating for a Digital Geneva Convention, the company explicitly positioned itself as a quasi-diplomatic actor (Hurel and Lobato 2018). Internally, it worked to develop whitepapers and policy documents aiming at broadcasting possible consensus areas for international cyber-norms development and established a Global Security Strategy and Diplomacy Team, which then gradually transformed into the Digital Diplomacy Team. States remain reluctant to the idea either because they deem private sector norms entrepreneurship illegitimate or due to the fact that if an initiative such as the Digital Geneva Convention is recognized, it might delegitimize previous government-led efforts to promote international norms for cyberspace—in particular, the UNGGE.

Having gone through an extensive list of documents, we were able to identify further forms of communication that perhaps set more clearly in the exercise of bringing coherence to the myriad of teams, programs and services—which we will explore in the last section. In publishing whitepapers and policy papers Microsoft publicizes their positions, provide an organized account of their strategy for policy engagement, and circulate their narrative for (i) cyber policy development and (ii) private sector inclusion (see Hurel and Lobato 2018). While this may be, at first, conceived as a "soft" approach to norms and policy making, documents range from general frameworks for cloud to frameworks for national cybersecurity strategy development, cyber-policy toolkits or even "mandatory" incident disclosure models (Microsoft, n.d.).

Creating a Narrative: The First Clouds in the Sky

> Against this backdrop, virtually every leading tech company found itself on the defensive in the summer of 2013. We conveyed our frustration to officials in Washington, DC. It was a watershed moment. It surfaced contrasts that have contributed to a chasm between governments and the tech sector to this day. Governments serve constituents who live in a defined geography, such as a state or nation. But tech has gone global, and we have customers virtually everywhere. The cloud has not only changed where and to whom we provide our services, it has redefined our relationship with customers. It has turned tech companies into institutions that in some ways resemble banks. People deposit their money in banks, and they store their most personal information—emails, photos, documents, and text messages—with tech companies. (Smith and Browne 2019, 22)

In 2014, as Satya Nadella took on the role as the CEO of Microsoft, he proposed a significant change in how the business operated. Back then he announced a new vision of what would promote a company-shift from a Windows-centric model to "mobile-first and cloud-first" model: "Microsoft is the productivity and platform company for the mobile-first, cloud-first world" (Nadella 2017, 54). Such a shift implied and enabled significant organizational, technological, and political changes—which spanned from diversifying cloud services to negotiating their public and private interests. One of the interviewees added that this change is, part and parcel, also a reflection of the need to innovate in a context where the company had gone from a global monopoly to sharing the stage with emerging technology companies. According to Nadella (2017), disputes such as the Microsoft versus United States, where the company challenged a warrant from the federal government to hand over e-mails that were originally stored in a server in Ireland, highlight the moral challenges that the company faced. Most importantly, it provides an interesting case for understanding the materiality of the services and infrastructures that not only support their operation as a platform and productivity company, but the social tensions and norms that are negotiated within and outside the company environment.

Interestingly, the company's narrative in cases such as this is one of exposing an inherent tension present in negotiating their role in the protection of individual "liberties of privacy and free speech and civil society requirements like public safety" (Nadella 2017, 112). However, it is also followed and informed by the development of strategies to further guide action. In Microsoft's case, this includes but is not restricted to the principle of designing trust in products and customers, partners, and governments. The "Redmond-based yet globally present" organizational structure is also an important feature to understanding how they claim legitimacy over their role in cybersecurity governance. As Brad Smith noted, "[t]he products and companies are far more global, and the pervasive nature of information and communications technology increasingly thrusts the tech sector into the center of foreign policy issues."

A second shift that followed from this "Windows-centric" to "cloud-first" model pertains to the relations of the company with governments. As one interviewee observed, for some time, some governments in Latin America were suspicious of the company for its monopoly on software services (and, accordingly, leveling up the pricing due to its comfortable position back then) and for its legal allegiance to the U.S. government, due to the fact that Microsoft is a U.S. company.[12] This has now changed, prompted by an increase in market competition, the loss of its monopoly of software production and distribution and by the attempts to carve out other market niches for the company (as the shift promoted by Mr. Nadella indicates). Not only did Microsoft need to "reinvent" themselves, they also had to convince governments that they could be *trusted* partners, which also depended on negotiating with their government interlocutors the need to establish transparency mechanisms and encode values, such as privacy, security, and trust, within their products.[13] This need becomes evident from one interview, held in October 2019, when it was said that if [Microsoft] could not show their clients and users (especially governments) that their products were safe, they would likely end up losing clients.

One such channel for building trust would be the company's transparency centers. Scattered in five different locations in Asia, Latin America, Europe, and the United States (there is no transparency center in the African continent to date), these centers allow governments access to source code and proprietary information from Microsoft's products and inspect them whenever there is suspicion about the products provided by the company. However, when we asked one of our interviewees about whether there was someone in the government of country *A*[14] that already requested access to the source code, the answer was negative (here, we could speculate whether this could be due to significant barriers in terms of availability of technical knowledge/skills to do this job within much of the already-short-of-resources branches of local and federal governments).

Transparency centers communicate one obvious expectation: that of trust, a value which is core to Microsoft's business model (Nadella 2017). Not only would these centers serve to expand dialogue with government interlocutors, they would also show the willingness of the company to open up itself to their scrutiny—of course, as long as certain requirements of confidentiality are met. Furthermore, in addition to being a channel of communication with government actors, Transparency Centers mobilize expectations around how "trust" with government actors should be practised (e.g., by means of granting access to—mostly illegible—proprietary information). For suspicious governments, in turn, "trust" becomes an important condition that will ultimately lead to either signing a contract or not. Since the shift to a cloud-based model and the resignification of its relationship with governments, not only is trust of fundamental importance to Microsoft's business model, its presence or absence is—at least, logically—core to the construction of spaces of negotiation.

As we have sought to show in this section, shared expectations of behavior are communicated through a multiplicity of channels—the legal text being only one of them, albeit the one that has received far more attention in specialized literature. In addition, we cannot detach the understanding of how these expectations come into being from the practical changes in business models and in the strategies that companies adopt to engage with governments. That is to say, we have emphasized here that through Microsoft's efforts to build themselves a legitimate space within norms-talk internationally, we can think of a different understanding of norm-building and cyber norms as part of a continuum in which the organizational and technological affordances in place matter as much as the negotiations undertaken to socialize the norm. In what follows, we will explore more of Microsoft's efforts to be seen as a "diplomatic" actor.

MICROSOFT, A DIPLOMATIC ACTOR?

As previously noted, private governance encompasses services and products, the maintenance of continuous organizational flexibility (new teams, posts) and key leadership influence. One dimension that has more recently gained considerable attention after the proposal for the Digital Geneva Convention is precisely how a global company such as Microsoft positions itself as a quasi-diplomatic actor. According to Brad Smith, his push toward diplomacy comes as one of the responses to the expansion of the company's global reach and rising concerns with cybersecurity: "The products and companies are far more global, and the pervasive nature of information and communication technology increasingly thrusts the tech sector into the center of foreign policy issues" (Smith and Browne 2019, 80). In order to advance their diplomatic engagement, the company works to influence global cybersecurity governance direct and indirectly. Engagement, in this front, relies mostly on the mobilization of staff within the company's Department of Corporate, External, and Legal Affairs (CELA)[15] and, most importantly, the Digital Diplomacy Team.

Microsoft works to advance multistakeholder and multilateral processes indirectly, whether through funding cybersecurity conferences,[16] participating in working groups,[17] attending international cybersecurity conferences or signaling support for norm entrepreneurship by others. When placed in a wider horizon on activities (indirect influence), the entrepreneurial efforts and cyber-norms documents of the company, the Digital Geneva convention is but one public-facing activity within a thread of continuous normative arrangements. Most notably, examples such as the Paris Call on Trust and Security and the Christchurch Call portray this cross-sector outward-facing norms engagement. However, members of the CELA Department also work continuously in providing inputs to specific multistakeholder cybersecurity processes. That is the case of the Internet Governance Forum,[18] where Microsoft has been continuously contributing to the work of the Best Practice Forum on Cybersecurity providing inputs to annual consultations. Within the Global Forum on Cyber Expertise, Microsoft has not only participated but also led—alongside government representatives—specific task forces on the implementation of cyber norms, Confidence-Building Measures and cyber diplomacy (see GFCE 2019).

Direct diplomatic engagement is equally central to the process of influencing the development of cyber norms as well as pushing for the broader participation within the private sector in cyber diplomacy. Even though from a tech sector standpoint, it might be indisputable that—as infrastructure providers and platform developers—a company such as Microsoft holds a considerable role in shaping and participating in global cybersecurity governance along with other tech giants, that is not necessarily the case when it comes to cyber-norms discussions. International processes such as the United Nations Group of Governmental Experts (UNGGE), whose main objective has been to discuss norms for responsible state behavior in cyberspace and, most recently, consider the applicability of international law in cyberspace. In light of fundamental immediate implications of any international negotiation such as the UNGGE, Microsoft has a direct interest mobilizing its resources to promoting norms to help mitigate and diminish cyberattacks and conflicts in an interdependent ecosystem such as cyberspace (see McKay et al. 2014; Charney et al. 2016; Nadella 2017; McKay 2018; Smith and Browne 2019).

Even though the company has maintained a long-standing relationship with different governments as part of their Government Security Programme, bilateral agreements or PPP, the international cyber-norms discussions presents a slightly different landscape (forums, initiatives) of interaction. Though bilateral and closed-meeting interactions are much more challenging to take into account in the study of how norms are built in practice, there is something to be said about how the company has expanded their engagement with governments. Be it on the "techplomacy" side, interacting with tech ambassadors from Denmark, Australia, and France, or creating a diplomatic cyber norms-oriented agenda to engage with governments bilaterally and multilaterally. One example worth noting was the Christchurch call, where Brad Smith narrates his encounter with New Zealand prime minister Jacinda Arden in March 2019, and how the Paris Call set a precedent back in December 2018 for thinking about a mechanism that could potentially bring governments, tech sector, and civil society together (Smith and Browne 2019). Cases such as this highlight an important feature of normative cascading effects of emerging cross-sector exchange—it also portrays how Microsoft diplomatic-focused interaction with governments has opened up avenues for their interaction with governments.[19]

Diplomatic efforts are not limited to strengthening ties with governments and/or socializing norms and principles in different multilateral fora, rather it entails circulating and developing norms *from* and *for* the private sector. That is the case of the Cybersecurity Tech Accord (CTA), a private sector-facing initiative launched in April 2018 that seeks to promote spaces for collective action, capacity building, and cooperation among global technology companies. The CTA also serves as a platform supporting other industry partners to onboard into cyber-norms discussions by (i) providing them the opportunity to attend consultations and conferences alongside governments and/or civil society and (ii) planning coordinated action and response to international processes (see Tech Accord 2019). Another example of peer-collaboration is the Global Internet Forum to Counter Terrorism (GIF-CT), an initiative established in early 2017 by Twitter, Facebook, Microsoft, and YouTube to deepen industry collaboration to combat terrorist abuse of platforms. Following the Christchurch Call, this group of companies has announced the creation of an independent initiative to work in a more structured setting with government and civil society organizations in preventing the exploitation of digital platforms by terrorists and violent extremist groups. Spaces such as this not only contribute as a coordination point, but serve as a knowledge and skills-sharing platform between sectors. However, such coordination and interaction contributes to the emergence of hybrid governance models that questions the differentiation between public and private roles and responsibilities.

The case of Microsoft's engagement with international cyber norms suggests that outcomes of corporate practices are not reducible either to the intentions of the individual human beings "behind it," nor do corporations act like independent beings with a life of their own. Instead, corporate action is more accurately seen as an aggregate of complex associations between internal policy and technical teams (which are more situated associations themselves), policy documents and initiatives, technologies and organizational infrastructures that support relations with governments and corporate customers, without which that what is called corporate action would look entirely otherwise (Latour 1994). This aggregate looks the way it does also because of the smaller associations that compose it and it is relevant to point out that each more complex association has an ontological status that is distinguishable from that of less complex ones.

Such a perspective over corporate norm entrepreneurship also allows us to bring in the commensurability of profit and rational action and normative and moral engagement. That is to say: when we look at how the company engages with governments, that is, through soft recommendations and attempts to influence policy making at either local, state, national, or international instances, or through mechanisms devised to "build trust" with state customers, we realize that, at once, companies can promote moral norms *and* seek profit. In Microsoft's case, what is pictured as norm promotion also has to do with what the company sees as an adequate use of for its products and services and may at times come as voluntary self-commitments with values—such as trust—deemed to be core to the reputation and afterlife of commercial and government solutions. As the relation between interests and moral values becomes more complex, it comes as no surprise then that the misuse of its software and hardware products, with attempts to exploit vulnerabilities in them, is among one of the company's primary concerns as it keeps advocating for some sort of accord among states.

Whereas there is a comprehensive assessment of how different private groups engage with international norms-making (Flohr et al. 2010; Rudder, Fritschler and Choi 2016; Strange 1992; Watkins 2007), this is a territory that still remains largely unknown to most studies on tech companies. Such a lack is nothing but problematic. Tech companies engage quite differently in regulating the behavior of its customers and users, and this has to do with the very nature of the services and products that are offered by them and how they work, are used, exploited, and transformed through practice. Indeed, some attention has been paid to how social media create community standards to bound what is an acceptable conduct on their platforms (Article 19, 2018) and regulate user behavior through technical (Musiani 2013) as well as legal (Belli and Venturini 2016) architectures. But these approaches remain mostly restricted to either self or individual regulation. Whereas they give us a hint on how companies—intentionally or not—develop sophisticated regulatory mechanisms through their products and services, they are less helpful once we try to make sense of the varied, sometimes conflicting or not-always-coherent-in-practice, organizational architectures underpinning such regulatory efforts. They are also not very helpful once we ask why and how companies engage with state actors to advocate for moral standards and common social codes of conduct to other actors beyond its peers in the private sector. Without in-depth discussion of why/how this happens, we foreclose our own understanding of how legitimacy is built through such efforts, as well as debates about how we should be dealing with these kinds of practices.

Adding to the burgeoning literature and policy initiatives to advance cyber norms (NATO 2013; McKay et al. 2014; Osula and Rõigas 2016; Finnemore and Hollis 2016; Charney et al. 2016; G7 2017; Nye 2018), Microsoft's call for a Digital Geneva Convention has drawn as much attention as suspicion to the company, as well as to its intentions and chances of succeeding. Whereas attention to corporate cyber-norms promotion and evaluations of its success or failure can be useful in assessing the efficacy (or not) of a situated initiative, both miss an important aspect of Microsoft's efforts: it is not—and, possibly, never was—about the Digital Geneva Convention. As our research on the company's organizational structure attempted to show, this is but one situated effort in the context of a diversified range of possibilities for political articulation undertaken by the company. As we sought to illustrate throughout this study, each particular relation begs the articulation of distinct policy strategies, infrastructures, and narratives that, in turn, constitute a multiplicity of associations in themselves—associations composed of people in policy teams, lobbying practices, technical systems, pieces of hardware, software, codes of conduct, different levels of government (local, state, national, and international), policy documents, physical installations, and so on. These associations point to the varied ways through which norms are articulated through corporate practice, some of them fairly straightforward, such as creating instruments of "soft influence," that is, policy papers and whitepapers, and producing advisory opinions, while some not so much—here, Transparency Centers are a case in point.

The empirical research suggests that such organizational complexity plays an important role in building legitimacy in private governance. This happens in—at least—three different ways. First, in devising strategies to deal with technical challenges to cyberspace security. As a platform and productivity technology company, Microsoft invests in the development of new technologies, software, and mitigation of incidents, such as the Conficker worm and the WannaCry ransomware, and also engages on combating cybercrime through its cybercrime unit.[20] This shaping of both the economic and technical dimensions of cybersecurity paves the way for private actors to be "recognized as legitimate by some larger public (that often includes states themselves) as authors of policies, of practices, of rules, and of norms" (Hall and Biersteker 2002, 4).

Second, in taking the lead in the proposal of a tech accord in the private sector and entering into cooperation with companies within and outside the tech sector, Microsoft has sought to establish itself as a moral leader among its peers. As Floh et al. (2010) note, establishing normative standards for its peers on the private sector is characteristic of corporate entrepreneurship. When engaging with norms promotion, corporations tend to work as meaning managers, establishing "new ways of talking about and understanding issues" (Finnemore and Sikkink 1998, 897). They may also support the setting or institutionalization of a new norm "by adopting a unilateral company code as best practice, by lobbying for it among its peers and by engaging in the creation of a collective self-regulatory initiative" (Flohr et al. 2010, 19) and play a role even after the norm has acquired some degree of institutionalization, by engaging with organizations supporting the norm and participation in revision processes (Flohr et al. 2010).

Third, by actively engaging with norms emergence beyond national borders, structuring public policy as well as diplomacy teams, regularly publishing policy documents aimed at state actors and getting involved in multilateral and multistakeholder policy processes, the company has clearly sought to stretch the boundaries of its legitimacy. Such stretching has less to do with the proposal of a Digital Geneva Convention in itself than with the company's aforementioned practices and organizational structure. That is to say, legitimacy building, at this stage, is better understood in terms of the complex associations and relations that follow from Microsoft's engagement with local, state, and national governments and its attempts to build legitimacy within the private sector and through its technical expertise.

The implications of this for the study of norms-making and power are manifold. The processual lenses hereto adopted suggest that power can be less straightforward than it seems: it can be distributed through internal teams, technical and policy considerations, expertise, "high-tech" centers, computational systems, soft-engagement. Consequently, what we call norms-making is equally distributed in these practices, stretching into every direction thanks to dynamic architecture of policy engagement. In this sense, norms-making cannot be understood as neither a state-only process, nor necessarily an actor-only process. By reintroducing private governance to the cyber-norms discussions—that is, looking at the strategies and associations involved in the establishing of a range of social codes of conduct—our goal was to provide an exercise of visualizing and further inquiring of what indeed, can pass as a norm. Initiatives such as a tech accord or a Digital Geneva Convention serve as important reminders that future cyber-norms and cybersecurity governance research needs requires careful unpacking.

CONCLUDING THOUGHTS ON CONTROVERSIES AND FURTHER RESEARCH

In this chapter, we sought to expand our previous research on private actor norm entrepreneurship in cybersecurity (Hurel and Lobato 2018) by undertaking an empirical analysis of the organizational structure of Microsoft. Through the analysis, we illustrated that not only questions of *who*—states? Nongovernmental organizations? Advocacy groups? Corporations?—produces norms matter, but also issues of *how* norms are made and *what* should be understood as norm-making processes in these analyses in the first place. This is a discreet albeit necessary step in the study of private governance in cybersecurity, as it opens up the field for entirely different and often extremely complex and messy ways of producing social codes of conduct—through technical means, soft influence, direct engagement with actors, and so on. Microsoft's case also shows that corporations can engage meaningfully and voluntarily with promoting and establishing socially accepted norms of conduct for both its peers and state actors at different levels of government—while also seeking to increase its profits and engaging with cost-benefits calculations. Thus, we can identify different dimensions stemming from the practices and associations constituted in and by corporate action, which include policy making, different degrees of advocacy (including lobbying), self-regulation and regulation through software and/or hardware.

By looking at the vast possibilities for associations—among documents, policies, teams, states, other corporations, high-tech infrastructures, techniques and technologies—we also highlighted three different dimensions of legitimacy building: technical/technological, among peers and multilateral/multistakeholder. Each form comes out of dynamic sets of associations, some more rigid, some more weak. What they tell us is that what is pictured as norm promotion is in fact a more complicated enterprise. By asking whether the Digital Geneva Convention proposal was actually novelty, we sought to illustrate that it is actually an actualization of these ever-changing associations. This is to say, it is a particular mode of producing norms, but not the only one, within Microsoft's organizational complexity.

One question that arises from the analysis is whether—despite the intense engagement with international norms promotion and the work of Transparency Centers as well as regional/national teams—the company still privileges its home country—the United States—as its main locus for policy making. Further research is still required about how the company develops relations with Global South countries and to what extent it is perceived by them as simply reproducing the interests of its "home country" or as something else. This could indicate whether the strength of particular associations at the expense of others might say something and potentially affect the company's advocacy. Distinctly, it could also shed a more clarifying light onto how local politics possibly shape long-term, global policies.

LIST OF INTERVIEWS

1. Interview, October 2019.
2. Interview, October 2019.
3. Interview, September 2019.
4. Interview, September 2019.

NOTES

[1] The authors would like to thank Prof. Dennis Broeders, Prof. Duncan Hollis, and Prof. Anna Leader for their support and invaluable comments to the development of this chapter. The authors would also thank the panel discussion held on "(Re) assessing the role of private actors in cybersecurity governance" at the ISA Annual Conference 2019, Toronto.

[2] In fact, the political role of companies has been widely debated within International Political Economy by means of discussions over multinational corporations. See: Strange (1991; 1996; 1998); Gill; Cutler (2014); Gilpin (1976); May (2015); Babic, Fichtner and Heemskerk (2017).

[3] Such as the 2019 Brazil-EU Consultations on Preventing Conflict in Cyberspace, the 2018 Conference Responsible Behaviour in Cyberspace: Novel Horizons and the new European framework for Cyber Sanctions.

[4] Notably, they are progressively becoming locus of attention. See, for example, Dunn Cavelty (2016) and Carr (2016).

[5] In this work, we also consider as IR studies in Global Governance and International Political Economy.

[6] This has also proven to be a challenge to the development of this chapter. In spite of having conducted interviews, analyzed public documentation, and engaged in participant observation across different events, the traceability of Microsoft's engagement and interests was an exercise in itself. The generativity and fast-paced change of the company's organizational structure allowed us to further understand that their engagement in diplomacy, policy and product development (enterprise side) is a continuous process of communication and internal negotiation. Norms are continuously challenged, reinforced, maintained, and transformed within complex arrangements

that do not necessarily imply in a clear-cut rational and objective response. Rather, they rely on internal alignments, leadership, and narrative-building.

7. However, in a far less explicit fashion than its peers (e.g., Facebook or Google) also due to different business models.

8. Executive security adviser at Microsoft Enterprise Cybersecurity Group.

9. See Smith and Browne (2019) chapter 5 note 2 for a detailed description of the development of the DCU since early 2000s.

10. The Cybersecurity Policy Framework, launched in 2018, holds together many of the previous documents directed to capacity building and development of national cybersecurity strategies. It serves as an interesting case for understanding how Microsoft gradually organized their agenda and positions on this particular area. Most importantly, they explicitly state the purpose of the document—and their aim in circulating it—that is, to provide "a high-level overview of concepts and priorities that must be top of mind when developing an effective and resilient cybersecurity policy environment" (McKay 2018).

11. Interestingly, in 2012, Microsoft developed an expected cybersecurity policy PPP timeline called "Cybersecurity Policy and Partnership Evolutionary Curve" that ranged from their early experiences in working with governments at the national level—risk management (2000) and resiliency (2005)—to new avenues for collaboration on cyber norms at the international level—starting from Internet governance (2010) to cybersecurity norms development (2015) and finally reaching harmonization (2020) (Thomlinson 2012).

12. Curiously, possibly in anticipation to this kind of criticism, one interviewee promptly emphasized the legal bond of the subsidiary in which s/he worked with the country in which it operated.

13. See Nadella (2017) and Smith (2019) for a detailed account of how both the president and CEO of the company portrayed the internal negotiations during the Snowden revelations and how they responded deciding to sue the U.S. government through the Foreign Intelligence Surveillance Court.

14. Where the subsidiary for which s/he works operates.

15. Regionally, the CELA Departments work to represent global principles and advocacy strategies in their respective countries.

16. Such as the Paris Peace Forum in 2018 (see Belin 2018), Global Commission on the Stability of Cyberspace, Global Conference on Cyberspace and others.

17. Such as the Best Practice Forum (BPF) on Cybersecurity within the Internet Governance Forum, or different Working Groups of the GFCE.

18. A global multistakeholder platform of the United Nations dedicated to facilitating the discussion of public policy issues related to the Internet.

19. In cyber norms-discussions (both internationally and regionally), Microsoft is perhaps the only industry representative participating in closed-door negotiations continuously. Though it is more challenging to generalize when it comes to interaction and influence in concealed environments, through participant observation the researchers were able to identify specific occasions where the company was the only industry partner represented either in multilateral negotiations or in closed multistakeholder environments. In early 2019, the EU Cyber Forum was followed by a closed civil society side meeting. Participants included civil society organizations, think

tanks, academics and Microsoft. Examples such as this illustrate not only the emerging spaces of interaction resulting from sustained engagement with global cybersecurity and cyber-norms community, but it creates an entry point for them to advocate, communicate and bring other industry sectors—such as those that are members of the CTA. All of which support the narrative echoed by Brad Smith of industry as technology providers and central to the promotion of peace and secure cyberspace.

20. The digital crime unit, in cooperation with academic experts and industry, successfully took down the Rustock botnet (Microsoft 2011) and further engaged in joint operations with the financial sector and law enforcement agencies—the most aggressive operation being Operation b54 (Boscovich 2013).

REFERENCES

Abbate, Janet. 1999. *Inventing the Internet.* Cambridge: MIT Press.

Abrahamsen, R., and M. Williams. 2009. "Security beyond the state: Global security assemblages in international politics". *International Political Sociology*, 3 (1): 7–17.

Article 19. 2018. *Facebook Community Standards: Legal Analysis*, June 2018. (Available at: https://www.article19.org/wp-content/uploads/2018/08/Facebook-Community-Standards-June-2018.pdf; accessed: Sept. 2, 2018.)

Assaf, D. 2009. "Conceptualising the use of public–private partnerships as a regulatory arrangement in critical information infrastructure protection". In: A. Peters, L. Koechlin, T. Förster, and G. Fenner Zinkernagel (eds.). *Non-State Actors as Standard Setters*, 61–83. Cambridge: Cambridge University Press.

Avant, Deborah D. 2005. *The Market Force: The Consequences of Privatizing Security*. Cambridge: Cambridge University Press.

Babic, Milan, Jan Fichtner, and Eelke M. Heemskerk. 2017. "States versus corporations: Rethinking the power of business in international politics". *The International Spectator*, 52 (4): 20–43.

Barrinha, André, and T. Renard. 2018. "Cyber-diplomacy: The making of an international society in the digital age". *Global Affairs*, 3 (4–5): 353–364.

Belin, Célia. "What the Paris Peace Forum tells us about France—and about the world". Brookings Institute. (Available at: https://www.brookings.edu/blog/order-from-chaos/2018/11/09/what-the-paris-peace-forum-tells-us-about-france-and-about-the-world; accessed: Oct. 21, 2018.)

Belli, Luca, and Jamila Venturini. 2016. "Private ordering and the rise of terms of service as cyber-regulation". *Internet Policy Review*, 5 (4). (Available at: http://policyreview.info/articles/analysis/private-ordering-and-rise-terms-service-cyber-regulation; accessed: 4 Sept. 2018.)

Berger, Peter L., and Thomas Luckmann. 1967. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge.* Harmondsworth: Penguin.

Berndtsson, Joakim, and Christopher Kinsey. 2016. *The Routledge Research Companion to Security Outsourcing*. London: Routledge.

Bevir, Mark. 2009. *Key Concepts in Governance*, 128–132. New York: SAGE.

Bies, Robert J., Jean M. Bartunek, Timothy L. Fort, and Mayer N. Zald. 2007. "Corporations as social change agents: Individual, interpersonal, institutional, and environmental dynamics". *Academy of Management Review*, 32 (3): 788–793.

Boscovich, Richard Domingues. 2013. "Microsoft works with financial services industry leaders, law enforcement and others to disrupt massive financial cybercrime ring". *The Official Microsoft Blog*. (Available at: https://blogs.technet.microsoft.com/microsoft_blog/2013/06/05/microsoft-works-with-financial-services-industry-leaders-law-enforcement-and-others-to-disrupt-massive-financial-cybercrime-ring/; accessed: Sept. 3, 2018.)

Bouwen, Pieter. 2002. "Corporate lobbying in the European Union: The logic of access". *Journal of European Public Policy*, 9 (3): 365–390.

Burt, Tom. 2018a. "Announcing the defending democracy program". Microsoft. (Available at: https://blogs.microsoft.com/on-the-issues/2018/04/13/announcing-the-defending-democracy-program/; accessed: Sept. 10, 2018.)

Burt, Tom. 2018b. "Protecting democracy with Microsoft AccountGuard". Microsoft. (Available at: https://blogs.microsoft.com/on-the-issues/2018/08/20/protecting-democracy-with-microsoft-accountguard/; accessed: Sept. 10, 2018.)

Burt, Tom. 2018c. "Defending against disinformation in partnership with NewsGuard". Microsoft. Available at: https://blogs.microsoft.com/on-the-issues/2018/08/23/defending-against-disinformation-in-partnership-with-newsguard/; accessed: Sept. 10, 2018.

Carr, Madeline. 2016. "Public–private partnerships in national cyber-security strategies". *International Affairs*, 92 (1): 43–62.

Charney, Scott, Erin English, Aaron Kleiner, Nemanja Malisevic, Angela McKay, Jan Neutze, and Paul Nicholas. 2016. "From articulation to implementation: Enabling progress on cyber security norms". Microsoft, white paper, June 2016.

Crouch, Colin. 2004. "Markets and states". In: Nash, Kate, and Alan E. Scott (eds.). *The Blackwell Companion to Political Sociology*, 240–249. Oxford: Blackwell.

Digital. n.d. "Digital crimes unit: Leading the fight against cybercrime". Microsoft, policy paper.

Dunn Cavelty, Myriam. 2016. "Cyber-security and private actors". In: Rita Abrahamsen and Anna Leander (eds.). *Routledge Handbook of Private Security Studies*. New York: Routledge.

Dunn Cavelty, Myriam, and Manuel Suter. 2009. "Public-private partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection". *International Journal of Critical Infrastructure Protection*, 2 (4): 179–187.

ENISA. 2017. *Public Private Partnerships (PPP): Cooperative Models*. ENISA. (Available at: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models; accessed: Sept. 6, 2018.)

FEC. 2018. "FEC approves advisory opinion and notification of availability". Federal Election Commission. (Available at: https://www.fec.gov/updates/fec-approves-advisory-opinion-and-notification-availability/; accessed: Sept. 6, 2018.)

Finnemore, Martha, and Duncan B. Hollis. 2016a. "Constructing norms for global cybersecurity". *Temple University Beasley School of Law. Legal Studies Research Paper* n. 52: 89–101.

Finnemore, M., and D.B. Hollis. 2016b. "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, and Sandra Schwindenhammer. 2010. *The Role of Business in Global Governance: Corporations as Norm-Entrepreneurs*. London: Palgrave.

Friedman, M. 2007. "The social responsibility of business is to increase its profits". In: W.C. Zimmerli, M. Holzinger, and K. Richter (eds.). *Corporate Ethics and Corporate Governance*. Berlin: Springer.

Fuchs, Doris. 2007. *Business Power in Global Governance*. Boulder, CO: Lynne Rienner.

G7. 2017. "On responsible states behavior in cyberspace". *Lucca*, 17 April 2017. (Available at: https://s3.amazonaws.com/ceipfiles/pdf/CyberNorms/Multilateral/G7+Declaration+on+Responsible+States+Behavior+in+Cyberspace+4-11-2017.pdf; accessed: Sept. 4, 2018.)

Garriga, Elisabet, and Domènec Melé. 2004. "Corporate social responsibility theories: Mapping the territory". *Journal of Business Ethics*, 53 (51): 51–71.

GFCE. 2019. "Report GFCE WG A—Task Force on CBMs and norms implementation & Cyber diplomacy". Global Forum on Cyber Expertise. (Available at: https://cdn.foleon.com/upload/17621/gfce_secretariat_wgm2019_wg_a_report.90f7333bc1c3.pdf; accessed: Oct. 22, 2019.)

Gill, Stephen, and Claire A. Cutler. 2014. "New constitutionalism and world order: General introduction". In: S. Gill (ed.). *New Constitutionalism and World Order*, 1–22. Cambridge: Cambridge University Press.

Gilpin, Robert. 1976. "Review: The political economy of the multinational corporation: Three contrasting perspectives". *The American Political Science Review*, 70 (1): 184–191.

Gorwa, Robert. 2019. "What is platform governance?" *Information, Communication & Society*, 22 (6), 854–871.

Gorwa, Robert, and Anton Peez. 2018. "Tech companies as cybersecurity norm entrepreneurs: A critical analysis of microsoft's cybersecurity tech accord". SocArXiv, working paper, December 11, 2018. (Available at: https://doi.org/10.31235/osf.io/g56c9.)

Government. n.d. "Government security program: An overview". Microsoft, policy paper.

Grigsby, Alex. 2017. "The end of cyber norms". *Survival: Global Politics and Strategy*, 56 (6): 109–122.

Hall, Rodney Bruce, and Thomas J. Biersteker. 2002. "The emergence of private authority in the international system". In: Rodney Bruce Hall and Thomas J. Biersteker (eds.). *The Emergence of Private Authority in Global Governance*, 3–22. Cambridge: Cambridge University Press.

Hurel, Louise Marie. 2016. "Cybersecurity and internet governance: Two competing fields?". *SSRN* (Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036855; accessed: Sept. 10, 2018.)

Hurel, Louise Marie. 2018. "Architectures of security and power: IoT platforms as technologies of government". MSc diss., London School of Economics and Political Science. (Available at: https://doi.org/10.13140/RG.2.2.28293.29920.)

Hurel, Louise Marie, and Luisa C. Lobato. 2018. "Unpacking cyber norms: Private companies as norms entrepreneurs". *Journal of Cyber Policy*, 3 (1): 61–76.

Kitchin, Robert. 2014. *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. Thousand Oaks, CA: SAGE.

Lapowski, Issie. 2018. "Tech giants are becoming defenders of democracy. Now what?" *WIRED*, Aug. 22, 2018. (Available at: https://www.wired.com/story/microsoft-facebook-tech-giants-defending-democracy/; accessed: Sept. 10, 2018.)

Latour, Bruno. 1994. "On technical mediation: Philosophy, sociology, genealogy". *Common Knowledge*, 3 (2): 29–64.

Latour, Bruno. 2005. *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford: Oxford University Press.

Leander, Anna. 2010. "Commercial Security Practices". In: P.J. Burgess (ed.). *Handbook of New Security Studies*. New York: Routledge.

Leigh Star, S., and K. Ruhleder. 1996. "Steps toward an ecology of infrastructure: Design and access for large information spaces". *Information Systems Research*, 7 (1): 111–134.

Lobato, Luisa. 2016. "Unravelling the cyber security market: The struggles among cyber security companies and the production of cyber (in)security". MSc diss., Pontifical Catholic University of Rio de Janeiro. (Available at: https://doi.org/10.17771/PUCRio.acad.27784.)

May, Christopher. 2015. "Who's in charge? Corporations as institutions of global governance". *Palgrave Communications*, 1: 1–10.

Mayntz, Renate. 2003. "New challenges to governance theory". In: Henrik P. Bang (ed.). *Governance as Social and Political Communication*, 27–40. Manchester: Manchester University Press.

McIntyre, Mark. 2017. "How public-private partnerships can combat cyber adversaries". Microsoft. (Available at: https://cloudblogs.microsoft.com/microsoftsecure/2017/12/13/how-public-private-partnerships-can-combat-cyber-adversaries/; accessed: Sept. 4, 2018.)

McKay, Angela. 2018. "Building on experience: A framework for cybersecurity policy". Microsoft, blog post. (Available at: https://cloudblogs.microsoft.com/microsoftsecure/2018/08/09/building-on-experience-a-framework-for-cybersecurity-policy/; accessed: Sept. 8, 2018.)

McKay, Angela, Paul Nicholas, Jan Neutze, and Kevin Sullivan. 2014. *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World*. Microsoft.

Microsoft. 2005. "Microsoft advocates comprehensive federal privacy legislation". Microsoft. (Available at: https://news.microsoft.com/2005/11/03/microsoft-advocates-comprehensive-federal-privacy-legislation/; accessed: Oct. 21, 2019.)

Microsoft. 2011. "Taking down Botnets: Microsoft and the Rustock Botnet". Microsoft corporate blogs. (Available at: https://blogs.microsoft.com/on-the-issues/201

1/03/17/taking-down-botnets-microsoft-and-the-rustock-botnet/; accessed: Sept. 2, 2018.)

Microsoft. 2014. "Microsoft government security program: Helping address the unique security requirements of national governments". Microsoft.

Microsoft, n.d. "Cybersecurity policy toolkit: Mandatory incident disclosure models". Microsoft. (Available at: https://www.microsoft.com/en-us/cybersecurity/content-hub/cybersecurity-policy-toolkit-mandatory-incident-disclosure-models; accessed: Sept. 1, 2018.)

Musiani, Francesca. 2013. "Governance by algorithms". *Internet Policy Review*, 2 (3).

Musiani, Francesca, Derrick L. Cogburn, Laura DeNardis, and Nanette Levinson. 2016. *The Turn to Infrastructure in Internet Governance*. London: Palgrave Macmillan.

Onuf, Nicholas G. 1989. *World of Our Making: Rules and Rule in Social Theory and International Relations*. Columbia: University of South Carolina Press.

Nadella, Satya. 2017. *Hit Refresh: The Quest to Rediscover Microsoft's Soul and Imagine a Better Future for Everyone.* New York: Harper Business.

Newman, Lily Hay. 2018. "How Microsoft tackles Russian hackers—And why it's never enough". *WIRED*, August 21, 2018. (Available at: https://www.wired.com/story/microsoft-russia-fancy-bear-hackers-sinkhole-phishing/; accessed: Sept. 4, 2018.)

Nye, Joseph. 2018. "How Will New Cybersecurity Norms Develop?" *The Strategist*, the Australian Strategic Policy Blog. (Available at: https://www.aspistrategist.org.au/how-will-cybersecurity-norms-develop/; accessed: Sept. 5, 2018.)

Osula, Anna-Maria, and Henry Roigas (eds.). 2016. *International Cyber Norms: Legal, Policy & Industry Perspectives*. Tallinn: NATO CCDCOE.

Plantin, Jean-Christophe, Carl Lagoze, Paul N. Edwards, and Christian Sandvig. 2016. "Infrastructure studies meet platform studies in the age of Google and Facebook". *New Media & Society*, 20 (1): 293–310.

Rönnegard, David (ed.). 2015. *The Fallacy of Corporate Moral Agency.* New York: Springer.

Rosenau, J. N., and E.-O. Czempiel (eds.). 1992. *Governance without Government: Order and Change in World Politics*. Cambridge, UK: Cambridge University Press.

Rudder, Catherine E., A. Lee Fritschler, and Yon J. Choi. 2016. *Public Policymaking by Private Organisations: The Challenges for Democratic Governance*. Washington: Brookings Institution.

Simos, Mark. 2018. "Cybersecurity reference architecture: Security for a hybrid enterprise". Microsoft. (Available at: https://cloudblogs.microsoft.com/microsoftsecure/2018/06/06/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/; accessed: Sept. 7, 2018.)

Smith, Brad, and Carol Ann Browne. 2019. *Tools and Weapons: The Promise and the Peril of the Digital Age*. New York: Penguin.

Smith, Brad. 2018. "Facial recognition technology: The need for public regulation and corporate responsibility". Microsoft. (Available at: https://blogs.microsoft.c om/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/; accessed: Sept. 9, 2018.)

Smith, Brad. 2017. "The need for a Digital Geneva Convention". Microsoft blogs. (Available at: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/; accessed: Sept. 9, 2019.)

Strange, Susan. 1998. *States and Markets*. San Francisco: University of California Press.

Strange, Susan. 1996. *The Retreat of the State: The Diffusion of Power in the World Economy*. Cambridge: Cambridge University Press.

Strange, Susan. 1991. "Big business and the state". *Millennium Journal of International Studies*, 20 (2): 245–250.

Tech Accord. 2019. "The cybersecurity tech accord response to a call for contributions from best practice forum working group on 'Cybersecurity Culture, Norms and Values'". Tech Accord. (Available at: https://cybertechaccord.org/category/policies-rfis/; accessed: Oct. 21, 2019.)

Thomlinson, Matt. 2012. "Cybersecurity norms and the public private partnership: Promoting trust and security in cyberspace". Microsoft. (Available at: https://cloudblogs.microsoft.com/microsoftsecure/2012/10/05/cybersecurity-norms-and-the-public-private-partnership-promoting-trust-and-security-in-cyberspace/; accessed: Sept. 9, 2018.)

Van Dijck, J. 2013. *The Culture of Connectivity: A Critical History of Social Media.* Oxford: Oxford University Press.

Wendt, Alexander. 2004. "The state as person in international theory". *Review of International Studies*, 30 (2): 289–316.

Wendt, Alexander. 1992. "Anarchy is what states make of it: The social construction of power politics". *International Organization*, 46 (2): 391–425.

Wendt, Alexander. 1995. "Constructing international politics". *International Security*, 20 (1): 71–81.

Westermann-Behaylo, Michelle K., Kathleen Rehbein, and Timothy Fort. 2015. "Enhancing the concept of corporate diplomacy: Encompassing political corporate social responsibility, international relations, and peace through commerce". *Academy of Management Perspectives*, 29 (4): 389.

Governing Cyberspace