Unpacking Cyber Norms: Private companies as norm entrepreneurs

Louise Marie Hurel
London School of Economics and Political Science

Luisa Cruz Lobato
Pontifícia Universidade Católica do Rio de Janeiro

Abstract: Concerns over practices in cyberspace are central to the consolidating international agenda for cybersecurity. Responses to such concerns come in different shapes and sizes, and are proposed by different actors. Whether it concerns intellectual property rights, the theft of trade secrets, collection of personal data, critical infrastructure protection, DNS security, or geopolitical issues, the rise of cybersecurity as a multifaceted global issue has led to the proliferation of governance mechanisms aimed at responding thereto. While state efforts have sought to promote norms of responsible state behaviour in cyberspace, we argue that technology companies are also taking the lead as norm entrepreneurs in the context of the stability and security of cyberspace. We explore the tensions between current literature on cyber norms and the role of private actors as potential norm entrepreneurs in global cybersecurity. In an attempt to determine the position of private actors in this field, we turn to practices such as corporate diplomacy and lobbying as avenues for highlighting the methods in which corporations engage in international policymaking in general, and cyber norms in particular. We look at Microsoft's case to unpack the company's role in the normative development of cybersecurity globally. We analyse documents containing the company's policies and strategies, and argue that these efforts consist of an attempt to influence global public policies on cybersecurity. In conclusion, we note that, notwithstanding these efforts, the lack of coordination between different aspects of norm-making processes illustrates the challenges facing the advancement of international cyber norms.

Key words: Cyber norms; Cybersecurity; Private Companies; Microsoft; Norms Entrepreneurship

Introduction

Concerns over practices in cyberspace are becoming central to the consolidation of an international agenda for cybersecurity. Responses come in different shapes and sizes, and are proposed by different actors. Whether it concerns intellectual property rights, the theft of trade secrets, collection of personal data, critical infrastructure protection, Domain Name System security, or geopolitical issues, the rise of cybersecurity as a multifaceted global issue has led to the proliferation of governance mechanisms aimed at responding thereto. Over the last few years, organisations such as the North Atlantic Treaty Organisation (NATO), the Association of Southeast Asian Nations' (ASEAN) and the Organisation for Security and Cooperation in Europe (OSCE) have all worked on the formulation of regional and global guidelines for state behaviour in cyberspace. Most of them are motivated by a concern with the increasing adoption of and incentives to engage in offensive practices, ranging from the use of malware in targeting adverse systems to state-sponsored misinformation campaigns (UNIDIR 2015; Osula and Rõigas 2016).

Cybersecurity is best understood as a *process* triggered by the practices of different actors, namely markets, think tanks, IT communities, governments, and security experts. In this context, states have a role to play in authorising and/or recognising market practices in the field, and do so by contracting out a wide range of services to companies, or sharing the management of a given issue without relinquishing its own participation. However, when Bruce Schneier (2000) echoed the message 'security is a process, not a product' in the early 2000s, he was not referring to states but to private companies (i.e. software manufacturers). Nonetheless, he went on

to say that 'security does not have to be perfect, but the risks have to be manageable' and that ‘products alone can't solve security problems’ (Schneier 2000).

By focusing on cybersecurity as a result of an interplay of practices among different stakeholder groups, we are able to (1) establish how private companies position themselves vis-à-vis the interests and practices of other actors interested in shaping and influencing what falls under the label of ‘cybersecurity’; and (2) understand the strategies they have devised for doing so.

International Relations scholars have sought to address both normative developments in the international system and the engagement of state and non-state actors in these processes (Risse and Sikkink, 1999; Hall and Biersteker, 2004). While cybersecurity has gained considerable notoriety within IR literature, it has received far less attention when it comes to the actors and processes involved in its governance. That is why we ask what the role is of corporate actors in cyber norm-making processes, and which strategies they have developed to make the case for a broader participation of the sector therein. While state-related efforts such as the United Nations Group of Governmental Experts (UNGGE), G7, G20, and OSCE have sought to promote norms for responsible state behaviour in cyberspace (Maurer 2011), we argue that technology companies have also increasingly been taking the lead as norm entrepreneurs in the stability and security of cyberspace.

The ICT industry has long been central to the development of Internet infrastructure, software, hardware, and cybersecurity solutions and services. However, ICT dependency is not only about innovation and economic development' (Neutze and Nicholas 2013, 4); it provides both benefits and challenges for those who rely on it – namely governments, users, and companies. Another concern is that commercial, mass-market ICT companies – and the underlying infrastructure used to develop and operate

them – have also served as targets of cyber conflict. This has lead to significant risks to users, and implies rising re-engineering costs across industry sectors. Governments usually look to the ICT industry to prevent, detect, respond to, and recover from cyber-attacks (Charney et al. 2016).

In this paper, ICT industry engagement in the governance of cybersecurity is illustrated by Microsoft. In February 2017 its CEO, Brad Smith, called for the establishment of a Digital Geneva Convention. The proposal falls under the attempt to consolidate international norms to guarantee greater transparency over states' actions in cyberspace, and protect non-state actors from intended and unintended consequences. While this particular event has been closely scrutinised, it should not be seen as a sole effort. The company has also published a series of documents – white papers, reports, blog entries – in which it sets the stage for industry participation in policy discussions. Through active engagement in norm development, Microsoft calls attention to role of the ICT industry as *first responders* while simultaneously highlighting the need for a *shared responsibilities* in addressing cybersecurity challenges (McKay et al. 2014; Charney 2016).

We turn to IR scholarship on norm development in order (a) to revisit the conceptualisation of norms entrepreneurship and (b) to understand how the role of private actors has been addressed in this literature. In doing so, we also engage in an interdisciplinary effort to make sense of how the existing literature either legitimises and/or delegitimises the participation of private companies' actions in international norms development specifically and, more broadly, global governance.

Private actors consist of different groups of actors that are not statist in nature, such as non-governmental organisations, for-profit organisations, academic institutions, research centres, groups of experts, and others. For the purposes of this paper, when

referring to private actors we are referring to a particular group within this category: market/corporate actors that either support Internet infrastructure or provide hardware, software services

We explore the tensions between current literature on cyber norms and the role of private actors as potential norm entrepreneurs in global cybersecurity. In an attempt to determine the position of private actors in this field, we turn to practices such as corporate diplomacy and lobbying as avenues for highlighting how corporations engage in international policymaking in general, and cyber norms in particular. Our argument is that through these practices, private actors seek to influence the course of international politics, portray themselves as legitimate stakeholders and, most importantly, promote changes in state behaviour.

Focusing on Microsoft's case, we seek to understand the nuances of the already-established debate surrounding private ordering, governance, and private sector's influence on international flows of capital and power. We pay particular attention to documents and statements from Microsoft representatives in order to make sense of the company's political engagement in the international construction of cyber norms, as well as its influence on global public policy more broadly. Moreover, we focus on Microsoft's efforts to promote a global tech accord, and argue that it provides us with a way of understanding the role of private actors in the normative development of global cybersecurity governance and cooperation.

We conclude that Microsoft's engagement in cyber norm promotion differs from typical corporate norm entrepreneurship. Not only does the company focus on changing the behaviour of states regarding global cybersecurity norms, but also seeks to stretch its own legitimacy beyond technical and economic services to influence international diplomatic efforts at the forefront of global cybersecurity debates.

The study of norms and cyber norms in International Relations

IR scholarly debates on norms are fruitful for our study in two different ways. Firstly, they provide us with an insight into how norms emerge and, in turn, how international norms affect domestic politics and vice-versa. Attention to norm emergence is relevant in that it allows us to visualise the different instances in which norm entrepreneurs might act and thereby have an influence on norm-making processes. Secondly, the discussion of transnational human rights networks sheds some light on the role of non-state actors as norm entrepreneurs – which will be important to our later discussion of the role of Microsoft in the promotion of cybersecurity norms. It sets the stage for looking at the way in which not only transnational advocacy networks and actors within international organisations contribute to the establishment of international norms, but also the role of profit-oriented actors.

One of the challenges for cybersecurity has been the asymmetry between expected behaviour and the lack of coordination among different sectors. Scholarly literature on norms has sought to understand how individual interpretations of right and wrong become collective expectations of a behaviour – 'proper behaviour' (Risse and Sikkink, 1999) – and how these, in turn, 'influence the behaviour and domestic structure of states' (Risse and Sikkink 1999, 7). Norms can serve different functions: to order and constrain behaviour (regulative norms); to create new actors, interests, and categories of action (constitutive norms); to resolve conflict 'in a non-violent fashion by structuring a discourse on grievances' (Kratochwil 1989, 249); or serve as standards of appropriate behaviour (Risse and Sikkink 1998).

At an international level, the UN has long tried to promote collective expectations of behaviour, be it the 2003 resolution on the 'Creation of a Global Culture of Cybersecurity' or the 2017 United Nations Group of Governmental Experts

(UNGGE). On a regional level, organisations such as the OAS, ASEAN, OSCE, and NATO have also been working on capacity building and regional cooperation within cybersecurity. However, state-centric responses are limited in promoting coordination between different sectors working within cybersecurity. As we will see in later sections, governance and norm development in cybersecurity – as in similar transnational challenges – require collective expectations to be built across the spectrum of actors.

Non-governmental organisations, advocacy networks, international organisations, and transnational corporations play an important role in influencing states' behaviour. They can act to alter a state's beliefs regarding issues such as women's rights, international trade, and cybersecurity (Finnemore and Hollis 2016) through rhetoric and other strategies such as lobbying, persuasion, and shaming (Keck and Sikkink 1998). The socialisation of human rights norms[1] has provided insight into how actors other than states – such as Transnational Advocacy Networks (TANs) – can work as networks of shared principled ideas that use information and beliefs to motivate political action (Keck and Sikkink, 1998).[2] The socialisation process can range from repression and initial denial of the norm to eventual compliance; the reverse process

[1] Risse and Sikkink (1999) identify three distinct types of socialisation processes that work together to socialise states that are not compliant with human rights norms: instrumental adaptation, argumentation, and habitualisation. These processes involve distinct phases, such as repression (in which governments simply prevent particular groups from gathering information about human rights violations), denial (which involves the refusal to recognise the validity of international human rights norms and a consequent unwillingness to submit to international jurisdiction), tactical concessions (in order to take international pressure off the government); and the gradual acceptance of the validity of international human rights norms until the state's behaviour becomes rule-consistent.

[2] This model is heavily influenced by the 'boomerang effect' developed by Keck and Sikkink (1998) to address the socialisation strategies through which NGOs bypass states and seek to put pressure on them from the outside.

consists of the internationalisation of domestic norms through the efforts of various kinds of norm entrepreneurs (Finnemore and Sikkink 1998).

The activities of norm entrepreneurs speak directly to the issue of how norms emerge. According to Finnemore and Sikkink (1998), norm emergence is the first stage of a norm's 'life cycle', and is born of norm entrepreneurs' attempts to convince states to embrace the new norm. If successful, this stage is followed by the state's socialisation of the norm with other states, which is motivated by a combination of pressure to conform and the desire of the state to enhance its international legitimation. This 'cascading' may lead to the internalisation of the norm as it acquires a taken-for-granted quality, and is no longer a matter for broad public debate. After this, the internalised or cascading norm can become a standard of appropriate behaviour against which other norms will either emerge or compete for support. It should be noted, however, that the completion of this process is not inevitable, as emergent norms may fail to reach a 'tipping point' (Finnemore and Sikkink 1998, 895).

Norm entrepreneurship also provides a framework through which IR scholars have begun to make sense of the participation of non-state actors in norm-making processes. Having outlined the way in which the norm-making process occurs, we now turn to how norm literature in IR perceives the role of private actors therein. This literature pays significant attention to how private and non-state actors participate in the distinct phases of the norm-making process. However, as we shall see below, corporate entrepreneurs – as private actors engaged with norm entrepreneurship are also known – tend to promote norms among their peers, which can indicate a turning point in the way IR views the participation of private actors in norm-making processes, to the extent that corporations also undertake norm promotion as a way of gaining legitimation to act in typically governmental fora.

Norms, cyber norms, and private actors

Despite the prominent role of the private sector in cybersecurity development (Dunn Cavelty 2016), norm-making processes in this area have been dominated by state-sponsored efforts to establish a common language for state acts in cyberspace (Kuebris and Badiei 2017). Nevertheless, the entanglement of the horizontal (stakeholder groups involved) and the vertical (hierarchy) dimensions in cyber norm production constitutes a regulatory framework that can neither be seen as a cohesive playing field nor reduced to a mere dialectic relationship between robust or tacit agreements. The complexity of cybersecurity governance settings thus indicates that focusing attention on state actors alone misses the framework of actors and practices involved in multiple cyber norm-making processes. On the one hand, it seems fairly reasonable to argue that private companies have a role to play in providing security services. On the other hand, however, the idea of corporations as diplomatic players capable of influencing global cyber norms can be perceived as controversial.[3]

Scholarship on norms has contributed to the study of global politics by pointing to the role of non-state actors in promoting and advocating for international norms (Keck and Sikkink 1998; Barnett and Finnemore 2004). More than that, it has also drawn attention to how private actors become involved in these processes (Deitelhoff and Wolf 2013; Flohr et al. 2010).

In this way, while IR scholars have suggested that non-state actors are part of norm-making processes**,** the literature on cyber norms often maintains a focus on the role of states (Kuerbis and Badiei 2017). For the purposes of this paper, taking for

[3] See Rudder, Fritschler and Choi (2016) for a thorough discussion of the role of private governance and its influence on public policymaking, especially with regards to the challenges facing transparency and accountability in this particular governance setting.

granted this notion of cyber norms is particularly problematic in the sense that it discounts the participation of a wider spectrum of actors, namely private actors (Aviram 2005). This section thus focuses on the role of private companies in setting norms within cybersecurity. Following a debate on corporate entrepreneurship, it shows that IR scholarship on norms and its greater focus on the role of corporate entrepreneurship in norm-making processes may have contributed to challenging this somewhat odd statist bias in cyber norm literature. We also provide an overview of how private actors have been portrayed in IR scholarship, and highlight a set of practices that characterise the influence of companies on norm-making processes.

Non-state actors play a fundamental role in shaping the structures, as well as the norms and rules, that guide and inform behaviour on the Internet. As such, many see the dynamics of cybersecurity as contrasting with other security issues, arguing that state actors struggle to establish authority in a sphere that has been strongly shaped by companies, individuals, and various not-for-profit organisations (Dunn Cavelty 2016).

The involvement of state actors in conflicts in cyberspace has been a source of concern for many actors whose business depends on the stability of the network (Charney et al. 2016). In proposing norms for both governments and industry, as well as developing stronger systems to deter state actors from targeting technology users, companies are adopting a more proactive position, aimed at establishing an understanding of what cybersecurity is (Dunn Cavelty 2015; 2016). As such, they have been increasingly taking up the position of norm entrepreneurs, laying the groundwork for a dialogue between private and state actors.

However, at the heart of the debates on international cyber norms lies the United Nations Group on Governmental Experts (UNGEE) and the challenges to international cooperation on cyberspace (Maurer 2011; Grigsby, 2017). The UNGGE was established

in order to discuss and develop 'norms, rules and principles of responsible behaviour of states, confidence building measures, and capacity building'.[4] The rise of cyber norms as an international inter-state concern is also reflected in outcomes from the G7, ITU (see Radu 2014), NATO and other international organisations. However, as Radu notes, 'the international institutional architecture for the governance of the cyberspace is dominated by a multiplicity of initiatives aimed at increasing cooperation at the international level, as well as by a *redefinition of the roles played by existent actors*' (Radu 2014, 4 emphasis added).

The failure of the 2016-2017 UNGGE group is perhaps one of the best indicators of the 'redefinition of roles' in proposing new cyber norms that are able to go beyond the recognition of international law as applicable to cyberspace - as achieved during the 2013 UNGGE. The governance of cybersecurity poses collective action problems and, as Finnemore suggests, 'negotiating treaties can be a slow and cumbersome process, ill-suited to fast-changing issues like cybersecurity and Internet governance. Governments may also not be the best or only actors to be making rules in this area since so much of the technology is in private hands' (Finnemore 2011, 90). The so-called failure on the cyber norms front has not only contributed to bolstering the debate on confidence-building measures (Grigsby 2017), but also opened up avenues for rethinking norm-making processes on an international level.

In IR, interest in private actors follows a long process of contesting the statist basis of IR theory, as well as its understanding of social reality (Ashley 1988; Hobson 2003; Walker 2006). From as early as the 1980s, a burgeoning academic interest in the growing interdependence between states and economies shed some light on the

[4] A/70/174

importance of multinational companies in IR (Keohane and Nye 1987; 1998; Hobson 2003). Scrutiny of the practices of private military companies (PMCs) in the 1990s consolidated the relevance, way beyond economic affairs, of such actors in world politics (Leander 2005; 2010; Avant 2005). The privatisation and commercialisation of security, be it through PMCs or big tech companies, suggests an expansion of the number of actors interested and engaged in the *politics of security*, and even an 'outsourcing of security' (Berndtsson and Kinsey 2016).

The level of attention paid to corporate norm entrepreneurship suggests that, in many areas, entrepreneurship by private companies has taken on an authoritative role, as well as regulatory functions previously ascribed to states. To the extent that a norm-entrepreneur engages in the early stages of a norm life cycle (Finnemore and Sikkink 1998), the rise of 'corporate social responsibility' and the establishment of codes of conduct and collective, self-regulatory initiatives in several policy areas, such as human rights, the environment, and combating corruption, have lead to increased awareness of the role of corporations in norm development processes.

Corporations may work as meaning managers, establishing 'new ways of talking about and understanding issues' (Finnemore and Sikkink 1998, 897). They can also support the setting or institutionalisation 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 institutionalisation by engaging with organisations supporting the norm, as well as participating in revision processes (Flohr et al. 2010).

Flohr et al. (2010) note that different motivations – whether strategic, i.e. avoiding state regulation, or ethical concerns, i.e. corporate responsibility – may lead to

this kind of entrepreneurship. Business actors may become involved in different governance arrangements, such as those still dominated by the public sector, multistakeholder initiatives, or pure instances of private self-regulation among business actors, without the direct participation of other stakeholders (Flohr et al. 2010).

Corporate norm entrepreneurship suggests that, in many areas, entrepreneurship by private companies has taken on an authoritative role, as well as regulatory functions previously ascribed to states. According to Schäferhoff, Campe, and Kaan (2009, 451), this is certainly true of public-private partnerships (PPPs). These partnerships form a type of hybrid governance whereby non-state actors (i.e. NGOs and transnational corporations) co-govern with state actors to provide a collective good in which they are engaged in authoritative decision making (see Hall and Biersteker 2002; Schäferhoff et al 2009).[5] But it is one thing to have the private sector's expertise and services, and quite another to deem them legitimate enough to engage in norm making.

The study of corporate norm entrepreneurship suggests that the main distinction between corporate norm entrepreneurs and 'classic' entrepreneurs is that the former aim for self-regulation and to establish normative standards for the business sector, in contrast to the latter - NGOs and epistemic communities - which aim to make states and business actors commit to the norms they promote. Corporate actors act mainly in the phase of norm emergence as norm entrepreneurs and regime proponents, and while NGOs usually seek to change the practices of states through discourse, lobbying, and shaming, companies start by changing their own behaviour, 'thus offering best practice

[5] They note that PPPs constitute a hybrid type of governance, in which non-state actors co-govern alongside state actors for the provision of collective goods [i.e. security], and adopt governance functions that have formerly been under the sole authority of sovereign states' (Schäferhoff 2009).

for imitation by other companies that may lead into collective self-commitments' (Flohr et al. 2010, 10).

Hence what is new about contemporary corporate entrepreneurship is that its involvement in governance structures today comes more in the form of voluntary self-commitments in reaction to public expectation, and less as a function of delegated tasks. Flohr et al. (2010) see in this a somehow quiet invitation to private actors to take responsibility for the provision of the public good. In this way, the suggested *unpacking of cyber norms* is also an attempt to question whether the developments in cyber norms might allow us to approach the debate on norm entrepreneurship in a more nuanced way. In the following section, we assess how Microsoft's advocacy of cyber norms can contribute to the study of the role of private actors in norm-making.

Microsoft: norm entrepreneur?

A couple of months before the meeting of the fifth UNGGE, Microsoft's Chief Legal Officer, Brad Smith, publicly called for a Digital Geneva Convention during the RSA conference in early 2017. He argued that state-led offensive operations in cyberspace had resulted in the growing costs of incident response and customer protection services for the private sector. As he noted, in February 14, 2017, in Microsoft's official blog: 'the time has arrived to call on the world's governments to implement international rules to protect the civilian use of the internet'.

However, it is important to put this proposal in the context of the broader array of Microsoft's policy-engagement initiatives. The company has sought to redefine its role in cybersecurity governance through a multi-layered approach that encompasses the development of *diplomatic* strategies on an international level and *active engagement* in recommending and influencing cyber policies. This includes the structuring of its 'Global Security, Strategy and Diplomacy Team' to develop white papers and guidelines

for examining the effect of political decisions on cybersecurity, the support of new forums for multistakeholder dialogue on cybersecurity (i.e. Global Commission on the Stability of Cyberspace), and private partnerships.[6]

Prior to the Digital Geneva Convention Proposal, Microsoft had been laying the grounds for policy and norm development in cybersecurity. Cyber norm proposals range from international norms to national cybersecurity strategies. They have also developed recommendations for policy-makers regarding cloud computing, city, and incident response cyber resilience, (Rison 2016). Not only have they proposed a new framework for international cybersecurity norms, but they have also followed up by engaging in *diplomatic* dialogues with different stakeholder groups – such as the United Nations and the International Committee of the Red Cross, and forums such as the RSA, the Black Hat Conference, the Munich Security Conference, the Internet Governance Forum (IGF), and others. In a 2013 white paper, and also in a blog entry of October 21, 2013, the company stressed the need for greater harmonisation of laws and standards, risk reduction, transparency, collaboration, and proportionality in cybersecurity (Microsoft 2013).

Across the spectrum of such norms and policy proposals (see Rison 2016), and more explicitly in the Digital Geneva Convention proposal, there is a common call to establish *shared responsibilities* within cybersecurity. The notion of shared responsibilities harks back to some of the criteria for PPPs, such as forging relationships with government and organization, drawing goals, and sharing the risks and responsibilities (Bexel and Mörth 2010). However, the challenge at the international

[6] i.e. The Global Internet Forum to Counter Terrorism created by Microsoft, Facebook, Twitter, and Youtube.

diplomatic level is one that transcends the notion of PPPs, and questions the role of Microsoft as a potential norm entrepreneur and diplomatic actor.

Focus on the coordination of the relationship between companies and public authorities is not new. Attempts by private companies to orchestrate relations with IGOs have also been referred to as *corporate diplomacy* (Asquer 2012), namely the set of practices adopted in order to advance corporate interests 'by negotiating and creating alliances with key external players including governments, analysts, the media and non-governmental organisations (NGOs)' (Watkins 2007). In the early years that followed the end of the Cold War, Susan Strange (1992, 1-2) pointed to significant structural changes with regards to the growing interdependence between world politics and economics. The consolidation of a global market economy placed states in a position where they had to consider creating incentives so that companies would remain within their territory. Nonetheless, firms had to go beyond their home markets and seek additional markets in order to maintain profits. This shift in the nature of the competition between states - further promoted by technological development - resulted in what Strange called 'a fundamental change in the nature of diplomacy', in which governments had to negotiate with firms and vice versa. Sassen's *broad* definition of *state-firm diplomacy* echoes the economic power - command of technology, ready access to global sources of capital, access to markets (see Sassen 1992, 5-6) - of private companies influencing policy decisions.

The challenge in understanding the role of private actors as norm entrepreneurs (despite their alleged success or failure) is one of comprehending the role of private governance in cybersecurity. Rudder, Fritschler and Choi (2016, 2) note that failure to recognise the role of private governance in public policymaking 'is to risk losing some of its contributions to providing high-level expertise needed for intelligent

policymaking today, responsiveness to technological change, networks to reduce the global governance gap, and alternatives to the state'. However, the potential outcome of recognising private governance in public policymaking is to frame private companies as a source of expertise, rather than actual stakeholders that are able to take part in the process of developing cyber norms.

Thus, the case for unpacking private actors as norm entrepreneurs is less about the newness of private sector engagement in corporate diplomacy, and more about the uneasiness surrounding how and why they should be deemed to be legitimate actors in cybersecurity norm-making processes. This highlights the somewhat intricate, paradoxical nature of private companies in cybersecurity. While acknowledging the importance of their role as service providers (hardware, software, technical knowledge), there is a push-back from recognising their potential engagement in cyber norms.

In this regard, the source of legitimate authority of private tech companies is measured in relation to their market share, the diverse array of their products, and their sustained innovative capacity to remain one of the big tech players in the datafication of social, economic and political life. A narrow understanding of corporate diplomacy stands for the enhancement of management tools, strengthening executive level diplomacy and creating value for shareholders (Henisz 2014).

As both a platform and productivity technology company, Microsoft has been investing in the development of new technologies, software, and mitigation tools for security incidents - i.e. Conficker worm and WannaCry ransomware - as well as engaging in combating cyber crime.[7] These are examples of the company's multiple

[7] In a blog entry of March 17, 2011, Microsoft shows how it established a digital crime unit which, in collaboration with academic and industry experts, successfully took down the Rustock botnet. Another entry, from June 5, 2013, shows how it further engaged in joint operations with the

strategies, on a technical level, to address what it perceives as major sources of insecurity in cyberspace. By shaping the technical and economic dimensions of cybersecurity, private actors are 'recognised 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 2004, 4). However, what seems to be the case is that, when it comes to cyber norms, there is a clear tension between economic and technical legitimacy on the one hand, and the international policy dimension of this legitimacy on the other.

One element of this tension concerns the relationship 'between hierarchies and markets, the common good and private profit, and the government and governance' (Bezell and Mörth 2010, 4); in other words, public-private partnerships (PPPs). Over the years, the company has also worked to strengthen PPPs for cybersecurity. Created in 2003, the Government Security Program (GSP) focused on developing and deploying more secure IT infrastructures. However, the Program has undergone changes, and now incorporates services such as controlled access to the source code of some products, vulnerability and threat intelligence to respond to security incidents, the sharing of technical information, data regarding cloud services and, most importantly, as noted in the company Policy Blog, the Transparency Centers. According to the company's news center, the Program can be interpreted as an early attempt to position Microsoft as a company at the forefront of providing cybersecurity services to both governments and international organisations (e.g. NATO). While the initiative is directed at technical solutions and data sharing activities, the evolution of the GSP and the incorporation of the Transparency Centers since 2014 further denote the entrenchment of the company in

---

financial sector and law enforcement agencies - the most aggressive operation being Operation b54.

cybersecurity governance on a national scale - i.e. USA, Belgium, Brazil, Singapore, and Mexico.

Within this framework, the 'grafting' of the Geneva Conventions can be interpreted as Microsoft's step towards an increased *role* not only in engaging in norm entrepreneurship, but stretching the boundaries of its legitimacy in multilateral and multistakeholder cybersecurity policymaking processes. Microsoft has not only remained attached to its roles in technical support, services, and expertise, but actively engaged in what is called the first stage of the norm cycle: norm emergence (Finnemore and Sikkink 1998).

Throughout 2017 the company attempted to convince a wider critical mass to embrace a tech accord in the face of growing skepticism with regards the possibility of the development of global cyber norms. The accord would build on a multilateral framework for international human rights, in order to respond to concerns over the consequences of a state-led escalation of offensive cyber operations against private sector activities and services, and individual safety in cyberspace (McKay et al. 2014). Skeptics of this suggestion argue that some of its current vulnerabilities result from reliance on insecure software; governments insist that there are many initiatives and frameworks already in place, and struggle to understand the added value of a Digital Geneva Convention (Ermert 2017).

Nonetheless, through these mechanisms Microsoft not only promotes global 'multilateral' cyber norms with a 'multistakeholder' implementation, as stressed in its blog on June 8, 2017, but strives to consolidate the role of the company as a *political* and *diplomatic* international player. The way Microsoft has engaged in politics seems to differ substantially from what other corporate entrepreneurs have done. Conversely to the typical engagement of corporate actors with norm entrepreneurship as self-

regulation, this case illustrates an engagement shaped both by a self-regulatory effort (namely using the company's best practices as a norm for other companies) *and* something closer to classic entrepreneurship, as it also - quite vehemently - aims to influence, and possibly change state behaviour in cyberspace.

Typically in domestic politics, companies struggle (i.e. lobby) to make sure that their business' interests and operations are ensured. This may as well translate into some sort of advocacy for more or less regulation on an issue, and in companies taking a stand and advocating for particular principles, such as privacy (Cook 2016). More often than not, such efforts come in the form of open opposition to or support for a given state action or policy.

In contrast with service-based companies, however, Microsoft operates mainly at the level of hardware and software production, and has repeatedly shown concern with potential uses and misuses of its products, as well as with the targeting of its systems by state-based cyber attacks. Such concern very likely shaped the company's advocacy of the principle of trust among stakeholders (Charney et al. 2016).

In establishing a diplomacy team, producing targeted policy papers, and calling for an international convention on cyberspace, Microsoft decided to speak the language of states, and deliberately extend the reach of its lobbying influence to actors beyond the sphere of self-governance and the governance of its peers in the private sector. This goes together with what Rudder, Fritschler and Choi (2016) have indicated in their effort to distinguish the private sector from self-governance, as the first would also involve the governance of others, with a clear public impact.

Lobbying has thus been devised as both an attempt to ensure the company's interests and as a governance effort with potentially transnational implications; as distinct from domestic settings, it aims to influence several legal systems at the same

time. In this sense, Microsoft's advocacy indicates that private regulation - via algorithms and terms of service - of service-based platforms and the self-regulatory efforts of corporate entrepreneurs are not the only areas in which companies may become involved in problems of order and change in international politics.

Attention to the distinct ways in which, beyond a focus on private regulation, companies become engaged in international politics has been lacking in the cyber norm literature, despite recognition of the company's efforts to create some normative ground for state actors (Finnemore and Hollis 2016; Grigsby 2017). To a certain extent, this may indicate that it remains largely state-centered, thus overlooking the specifics of Microsoft's engagement with cyber norms.

Microsoft engages in different layers of cybersecurity nationally and globally. Transparency Centers, the Digital Geneva Convention proposal, and infrastructure services (e.g. cloud services) tie the company's socio-technical and multifaceted approach to regulating cybersecurity together. Technically, this engagement happens through incident response, botnet takedown operations, and technical support. Politically, it happens through norm entrepreneurship activities set forth by its 'Global Security Strategy and Diplomacy Team', as well as through international initiatives such as the Global Commission on the Stability of Cyberspace (GCSC). The company's Diplomacy Team engages in the promotion of global 'multilateral' cyber norms with 'multistakeholder' implementation, thus advocating for a stronger governmental commitment to global cybersecurity governance and norm entrepreneurship.

Developments across the spectrum of dimensions highlighted above show the deepening contribution of Microsoft not only to the global debate on cyber norms, but

as part of an internal process of redesignating the political expression of the company as a quasi-diplomatic entity and building up a socio-technical approach to cybersecurity governance on both a national and international level. Furthermore, they illustrate what happens when private actors willingly start to carve out a space in a typically statist sphere. In this, interestingly enough, Microsoft's case is not so much indicative of a successful cyber norm enterprise, but of another window that is slowly opening for private actors in the norm debate. Whether norm advocacy is successful or not, i.e. whether states buy into the spirit of the Geneva Convention proposal or similar, Microsoft's case may already offer some sort of precedent to other companies.

Conclusion

In this paper, we sought to explore how Microsoft has engaged in the promotion of international cyber norms. The IR literature on norms, in its growing focus on private actors from the mid-1990s onwards, has provided the theoretical ground for us to contextualise, situate, and understand the company's engagement with cyber norms and, in parallel, to understand existent conceptualisations of the role of corporate actors in norm creation and development. In this sense, while the literature on cyber norms remains too focused on the role of states, the failure to develop mechanisms at this level has contributed to a new context in which new forms of action are possible. The call to unpack cyber norms hereto advanced can best be understood as an attempt to go beyond a state-centric narrative and return to the question of understanding cybersecurity governance as an open playing field.

We recognise that analysing Microsoft’s role as a norm entrepreneur hardly captures the different ways in which the private sector engages in norm construction. The effect of Microsoft’s norm entrepreneurship in the form of proposing a Digital Geneva Convention (*norms cascading*) remains to be seen. Nonetheless, this case

shows that multiple paths can be taken by corporate actors in norm promotion, and can involve strategies that have been partially neglected in specialised literature to date. Microsoft's strategy has consisted of engaging in different layers of cybersecurity: national, regional, and global, through corporate diplomacy (i.e. norm entrepreneurship), and through the Diplomacy Team and the Global Commission on the Stability of Cyberspace, technical initiatives, and PPPs (i.e. Transparency Centers, incident response, and joint botnet takedown operations with governments and other companies).

Microsoft's case indicates that there is a dimension of corporate entrepreneurship that is yet to be understood by IR norm literature. Instead of focusing on influencing the behaviour of its 'peers' it has sought, through several of its diplomatic (and, to some extent, technical) policies, to play a role in influencing the behaviour of states, and in positioning itself as a relevant stakeholder in international cyber policy discussions.

IR literature and the study of private actors in global affairs could benefit not only from analysis of Microsoft's case, but also from the overall engagement of actors, and the dynamics and concerns surrounding cybersecurity. Among other things, the experience of cybersecurity can provide important reflections on governance challenges in the current international system. The lack of coordination between different agents in cyber norm-making processes – states, international organisations, and private companies – is particularly illustrative of the present challenges faced by the promotion of an international normative framework in cybersecurity governance. However, whether Microsoft is successful in its efforts or not, it may likely already offer a precedent not only to other IT companies, but to corporate actors from other fields as well.

We hope to contribute to the expansion of the scope of the debate surrounding norms and cybersecurity governance through an interdisciplinary approach. IR has produced extensive literature on the relation between norm development and diffusion, and could contribute to enhancing the understanding of the global dynamics of cybersecurity governance - and their correlation to local and regional dynamics. The literature on cybersecurity governance should take into account a host of different actors engaged in cybersecurity practices, as well as their ways of interacting *within* and *across* different stakeholder groups. As Finnemore and Sikkink (1998) argue, norms oscillate within the spectrum of robustness and flexibility, and do not necessarily take the form of legally binding agreements. This is to say that, while we decided to focus on the role of private actors, future research should also aim to explore the spectrum of non-state actors within cybersecurity governance norms. Civil society's role in this debate could provide a case in point, as it is still highly fragmented and ill-defined.

Private actors have been considered central to cybersecurity. Nevertheless, this recognition also comes at the high cost of contention vis-à-vis the perceived notion of cybersecurity as a traditional national security asset. In the case of norms, the idea of the state as a preconceived legitimate actor in norm production has long been perpetuated as 'normal' in traditional IR literature. While this is not an either/or question (either the state or private sector), it does help us to understand that norms are not produced in a vacuum, but are contested and legitimised in specific contexts (Finnemore and Hollis 2016).

Acknowledgements

The authors would like to thank the GigaNet Symposium 2017 for providing us with fruitful discussion and feedback on the preliminary versions of this work, in particular to Carolina Aguerre. We would also like to thank Emily Taylor and two anonymous reviewers kindly for fundamental comments that helped us as we were editing.

References

Avant, Deborah. 2005. "Private Security Companies." *New Political Economy* 10 (1): 121-131.

Aviram, Amitai. 2004. "Network Responses to Network Threats: The Evolution into Private Cyber-Security Associations." *Public Law and Legal Theory Working paper no.115*. Florida State University College of Law.

Ashley, Richard. 1988. "Untying the Sovereign State: A Double Reading of the Anarchy Problem." *Millennium - Journal of International Studies*, 17 (2): 227-262.

Asquer, Alberto. 2012. *What is Corporate Diplomacy?* SSRN. http://dx.doi.org/10.2139/ssrn.2009812

Barnett, Michael, and Finnemore, Martha. 2004. *Rules for the World: International Organizations in Global Politics*. Ithaca: Cornell University Press.

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

Bexell, Magdalena, and Mörth, Ulrika. 2010. *Democracy and Public-Private Partnerships in Global Governance.* New York: Palgrave Macmillan.

Charney, Scott, English, Erin, Kleiner, Aaron, Malisevic, Niemanja, McKay, Angela , Neutze, Jan, and Nicholas, Paul. 2016. "From Articulation to Implementation: Enabling Progress on Cyber Security norms." White paper. Microsoft: June.

Charney, Scott. 2016. "In it Together – Developing Cybernorms is a Shared Responsibility." *The Security Times*, February 2016. Accessed 10 March 2018 https://blogs.microsoft.com/eupolicy/2016/02/12/in-it-together-developing-cybernorms-is-a-shared-responsibility/

Cook, Tim. 2016. "A Message to Our Customers." *Apple Inc.*, February 16, 2016. Accessed 10 March 2018 https://www.apple.com/customer-letter/

Deitelhoff, Nichole, and Wolf, Klaus Dieter. 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, Kathryn Sikkink, and Stephen C. Ropp, 222-238. Cambridge: Cambridge University Press.

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

Dunn Cavelty, Myriam. 2015. 'The Normalization of Cyber-International Relations.' In *Strategic Trends 2015: Key Developments in Global Affairs*, edited by Oliver Thränertand Martin Zapfe. E. CSS.

Dunn Cavelty, Myriam. 2016. "Cyber-Security and Private Actors." In *Routledge Handbook of Private Security Studies*, edited by Rita Abrahamsen and Anna Leander, 89-99. New York: Routledge.

Ermert, Monika. 2017. "A Digital Geneva Convention: Nobel Prize-Worthy or Dangerous?" Intellectual Property Watch, 19 december. Available at: https://www.ip-watch.org/2017/12/19/digital-geneva-convention-nobel-prize-worthy-dangerous/

Finnemore Marta. 2011. "Cultivating International Cybernorms." Chapter 6 in *America's Cyber Future: Security, Prosperity in the Information Age*, edited by Kristin M. Lord and Travis Sharp. Washington DC: Center for a New American Security. Accessed 10 October 2017. http://citizenlab.org/cybernorms2011/cultivating.pdf.

Finnemore, Martha, and Hollis, Duncan B. 2016. *Constructing Norms for Global Cybersecurity*. Temple University Beasley School of Law. Legal Studies Research Paper n.52: 89-101.

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

Flohr, Annegret, Rieth, Lothar, Schwindenhammer, Sandra, and Wolf, Klaus D. 2010. *The Role of Business in Global Governance: Corporations as Norm-Entrepreneurs*. London: Palgrave Macmillan.

Grigsby, Alex. 2017. "The End of Cybernorms". *Global Politics and Strategy* 56 (6): 109-122.

Hall, Rodney B., and Biersteker, Thomas J. 2002. *The Emergence of Private Authority in Global Governance*. Cambridge: Cambridge University Press.

Henisz, Witold J. 2014. *Corporate Diplomacy: Building Reputations and Relationships with External Stakeholders*. Sheffield: Greenleaf.

Hobson, John M. 2003. *The State and International Relations*. Cambridge: Cambridge University Press.

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

Keohane, Robert, and Nye, Joseph. 1987. "Power and Interdependence Revisited." *International Organization* 41 (4): 725-753.

Keohane, Robert, and Nye, Joseph. 1998. 'Power and Interdependence in the Information Age.' *Foreign Affairs*, September-October. Accessed 10 January 2018. https://www.foreignaffairs.com/articles/1998-09-01/power-and-interdependence-information-age

Kratochwil, Friedrich V. 1989. *Rules, Norms and Decisions*: O*n the Conditions of Practical and Legal Reasoning in International Relations and Domestic Affairs*. Cambridge: Cambridge University Press.

Kuebris, Brenden, and Badiei, Farzaneh. 2017. "Mapping the Cybersecurity Institutional Landscape." *Digital Policy, Regulation and Governance* 19 (6): 466-492. https://doi.org/10.1108/DPRG-05-2017-0024

Leander, Anna. 2005. "The Market for Force and Public Security: The Destabilizing Consequences of Private Military Companies." *Journal of Peace Research* 42 (5): 605-622.

Leander, Anna. 2010. 'Commercial Security Practices.' In *Handbook of New Security Studies*, edited by Peter J. Burgess, 208-216. New York: Routledge.

March, James G., and Olsen, Johan P. 1989. *Rediscovering Institutions*: *The Organizational Basis of Politics*. New York: Free Press.

Maurer, Tim. 2011. *Cyber Norm Emergence at the United Nations—an Analysis of the UN's Activities Regarding Cyber-Security*. Belfer Center for Science and International Affairs.

McKay, Angela, Nicholas, Paul, Neutze, Jan, and Sullivan, Kevin. 2014. *International Cyber Security Norms: Reducing Conflict in a Internet-Dependent World*. White paper. Microsoft: December.

Microsoft. 2013. *Five Principles for Shaping Cybersecurity Norms*. White paper. Microsoft Corporation.

Microsoft. 2014. *Microsoft Government Security Program: helping address the unique security requirements of national governments*. Microsoft.

Neutze, Jan, and Nicholas, Paul. 2013. "Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms." *Georgetown Journal of International Affairs:* International Engagement on Cyber III: State Building on a New Frontier (2013-14), 3-15. Washington DC: Georgetown University Press.

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

Onuf, Nicholas G. 2008. *International Legal Theory: Essays and Engagements 1966-2006*. London: Routledge.

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

Portnoy, Michael, and Goodman, Seymour. 2009. *Global Initiatives to Secure Cyberspace: An Emerging Landscape*. Berlin:| Springer

Radu, Roxana. 2014. "Power Technology and Powerful Techologies: Global Governmentality and Security in the Cyberspace." Chapter 1 in *Cyberspace and International Relations: Theory, Prospects and Challenges*, edited by Jan-Frederik Kremer and Benedikt Müller. Berlin: Springer.

Rison, Alice. 2016. "Microsoft Incident Response and shared responsibility for cloud computing." *Microsoft Azure*, April 14. https://azure.microsoft.com/en-us/blog/microsoft-incident-response-and-shared-responsibility-for-cloud-computing/

Risse, Thomas, and Sikkink, Kathryn. 1999. “The Socialization of International Human Rights Norms into Domestic Practices: Introduction.” In *The Power of Human Rights: International Norms and Domestic Change*, edited by Thomas Risse, Stephen C. Ropp, and Kathryn Sikkink. Cambridge: Cambridge University Press.

Risse, Thomas, and Ropp, Stephen C. 1999. “International Human Rights Norms and Domestic Change: Conclusions.” In *The Power of Human Rights: International Norms and Domestic Change*, edited by Thomas Risse, Stephen C. Ropp, and Kathryn Sikkink. Cambridge: Cambridge University Press.

Risse, Thomas, and Ropp Stephen C. 2013. “Introduction and overview.” In *The persistent power of human rights: from commitment to compliance,* edited by Thomas Risse, Kathryn Sikkink and Stephen C. Ropp. Cambridge: Cambridge University Press

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

Schäferhoff, Marco, Campe, Sabine, and Kaan, Christopher. 2009. “Transnational Public-Private Partnerships in International Relations: Making Sense of Concepts, Research Frameworks, and Results.” *International Studies Review* 11 (3): 451-474.

Schneier, Bruce. 2000. “The Process of Security.” *Schneier on Security*. April. Accessed https://www.schneier.com/essays/archives/2000/04/the_process_of_secur.html

Strange, Susan. 1992. “States, Firms and Diplomacy”. *International Affairs* 68 (1): 1-15.

UNIDIR. 2015. “International Law and State Behaviour in Cyberspace” Series. *Compendium of Regional Seminars*. United Nations Institute for Disarmament Research.

Watkins, Michael D. 2007. “The Rise of Corporate Diplomacy (Finally!)”. *Harvard Business Review*. Available at: https://hbr.org/2007/05/the-rise-of-corporate-diplomac

Walker, R. B. J. 2006. “Lines of Insecurity: International, Imperial, Exceptional.” *Security Dialogue* 37 (1): 65-82.

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