Regulation of Cybersecurity: Power of Private Companies

Microsoft's Engagement with Diplomatic Processes in the Field of Cybersecurity

Universiteit Leiden

Master Thesis Crisis & Security Management

Written by: Lucia Morvicová

Student Number: s1682784

Supervised by: Dr. D.W.J. Broeders

Second reader: Dr. J. Matthys

Word Count: 17 983

Leiden University

Faculty of Governance and Global Affairs

Contents:

Abstract

States, the actors primarily responsible for arranging the majority of international regulatory regimes, have so far been unable to reach a consensus on how to govern international cyberspace. For example, in 2017, the UNGGE, arguably the most promising state-led effort to create international norms for cyberspace, did not prove to build on the previous two successful reports and failed. As a consequence, an increasing trend in the management of cyberspace through a norm-development advocated by tech companies has been recently taking place within the field of cybersecurity.

Acknowledging the emerging diplomatic role of private actors in cyberspace, the question that will guide this research is: *Does Microsoft's engagement with diplomatic processes on (the stability) of cyberspace conform to the theoretical model of club diplomacy and/or are we witnessing a shift towards a model of network diplomacy in this area of international politics?* The two initiatives which will be the focus of the research are Microsoft's Digital Geneva Convention and the Paris Call for Trust and Security in Cyberspace. The reason behind the choice of Microsoft as a case study is to analyze how private actors become involved with diplomatic processes in the field of cybersecurity.

1. Introduction

1.1 Regulation of Cyberspace and Emerging Challenges to Diplomacy

"Tech companies, with Microsoft at the forefront, are becoming the primary international legislators in cyberspace" (Kilovaty 2019a). This is due to their growing vulnerability in cyberspace, particularly because of state-sponsored activity online, which ultimately resulted in norm-building campaigns for safe cyberspace advocated by the private sector (ibid.). Statements similar to these have been recently expressed in some academic articles, but mainly put forward in a number of cyber-related blogposts and news articles and sparked controversy. Despite the growing amount of related titles, the validity of these claims is still contested by the academia as well as by states, the primary actors responsible for regulating the international order.
Recently, a considerable literature has grown up around the theme of cybersecurity and the relevant roles of different actors within this field. Private actors aim to pursue their interests in securing the cyberspace as the threat of state-sponsored cyber attacks has been growing. Such activity, in consequence, has a negative impact not only on the critical infrastructure that is owned by these private actors but also on the civil society, the main clients of the private sector. In this context, tech companies attempt to take lead on the governance of cyberspace as a response to the under-regulated state behaviour in cyberspace.

Another reason why technology companies enter the field of norm-entrepreneurship are the conflicting opinions expressed by states on the regulation of cyberspace, namely by the United States and Russia (Grigsby 2017, 114). These have been expressed over the past two decades and recently during the last round of the UNGGE process, arguably the most promising state-led process on the development of norms for cyberspace. During its last session in 2017, fundamental disagreements among the Group's 25 members emerged, specifically on the right to self-defense and the applicability of the International Humanitarian Law to cyber conflicts (Soesanto and D'Incau 2017). Against this backdrop, the last session of UNGGE did not build on its previous success and failed to release a consensus report (Ibid.). Moreover, the UNGGE process split into two parallel processes, one led by the United States (GGE), the other pursued by Russia (OEWG) (Grigsby 2018). This development, however, may split the General Assembly's attention on the issue, creating two exclusive clubs, where reaching a common consensus might become almost impossible (Ibid.)

Regulation of Cybersecurity: Power of Private Companies

Returning to the subject of private cybersecurity governance, the doubt arises as private actors attempt to take onto tasks that are predominantly the prerogative of states. In this vein, some states regard the infiltration of the private sector with suspicion as they fear that their legitimacy may be endangered (Badie 2018, 99). Overall, private actors are seen as unelected and unaccountable players whose sources of legitimacy are different from the ones of the state parties (Cooper, Heine and Thakur 2013, 11). In the end, the involvement of private tech companies in norm-building campaigns not only impinges upon the sovereignty of nation states but also challenges the traditional diplomatic practice.

It needs to be remained that matters regarding international law are the prerequisite of nation states, where states are the only legal actors who have the power to form and implement international rules (Badie 2018, 99). When it comes to norm-building initiatives, even though the involvement of the private sector is visible, states are not welcoming these actors as they wish to hold the upper hand over the international order (Ibid., 91). A good example is the UNGGE, a state-led process whose purpose is to establish guiding norms for responsible state behaviour in cyberspace. In general, it is not common for state actors to become signatories to initiatives coming from the private sector. However, multi-stakeholderism underpins the shared responsibility that state and non-state actors have on a given matter, in this case cybersecurity. Paris Call for Trust for Security and Cyberspace is one such initiative that emphasizes the multi-stakeholder approach, where both state and non-state actors participate in the development of norms suitable for all actors dependent on the Internet.

With respect to the field of diplomacy, cyber-norms building process goes beyond the traditional diplomatic practices given the unique attributions of cyberspace that do not fall under the internal affairs of any state (Mačák 2019, 82). Furthermore, the globalisation process produced a plurality of actors that some authors see as a fundamental transformation in the diplomatic relations of major powers (Cooper, Heine and Thakur 2013, 8; Heine 2013,54). In this respect, within the field of cybersecurity, diplomacy in its traditional terms is being challenged by the entrance of new non-state actors whose roles can be in some instances considered as diplomatic ones.

In order to fully understand the current dynamics between all actors in the field of cybersecurity, the diplomatic theory will be addressed. According to Pigman, diplomacy can be understood as the management of international relations by negotiation (Pigman 2018, 74). For

the purpose of this study, two different variations of diplomacy will be distinguished, namely the club and network diplomacy. The classical diplomacy, also referred to as the club model of diplomacy is based on the principles of top-down administration and command-and-control organization (Heine 2013, 58). More precisely, the main actors in this model of diplomacy are states where the interaction is limited only to accredited diplomats organized in a hierarchical structure (Ibid., 60). On the other hand, the network model of diplomacy emphasizes the myriad of actors at play in international interactions and involves actors that were traditionally kept out of the inner circles of diplomacy and policy negotiation (Cooper, Heine and Thakur 2013, 22) As a consequence, the network model brings together actors from various fields with different interests and engagement.

Nowadays diplomacy engages in wider processes of negotiation with transnational firms, civil society, and NGOs, all of which aim to reach a compromise on international political matters (Ibid.). The same can be said about the diplomacy of cyberspace where a plurality of actors that are dependent on each other interact. It is however uncertain which model of diplomacy is leading in explaining current developments within the field of cybersecurity. To clarify this matter, the thesis will study the case of Microsoft's engagement with the cyber diplomatic processes through which the thesis will analyse which model of diplomacy (i.e. club or network) explains the current developments in cyberspace best when it comes to actor participation.

The most politically active private player in the field of cybersecurity has been Microsoft which has since 2014 called for the advance of cyber norms and positioned itself as the spokesperson for several tech firms in the cybersecurity debate (Gorwa and Peez 2018, 12). In early 2017, the company's Chief Legal Officer Brad Smith called for the Digital Geneva Convention (DGC), an initiative to protect cyberspace through norm-development, multi-stakeholder approach and successful cooperation between the public and the private sector. However, this initiative faced several criticisms from governments as well as from academia. Majority of these criticisms has been raised by the governments who perceive the private sector as an unwelcome guest in the international arena as well as the fact that the proposal itself picks and chooses principles of the International Humanitarian Law which it adapts to its convenience (Badie 2018, 99; Llorente 2018).

Nevertheless, Microsoft continues to influence the political community through other

initiatives, namely the Cybersecurity Tech Accord and the Paris Call for Trust and Security in Cyberspace, which Microsoft jointly drafted with the French government (Matsakis 2018). Contrary to the DGC, the Paris Call is perceived as a success as it has been endorsed by over 60 governments and supported by more than 300 private companies. In this context, the progress Microsoft has made in affirming its role in the field of cyber diplomacy will be studied by this thesis. This will be done by comparing the two initiatives (i.e. DGC and Paris Call) to each other, thus distinguishing the Paris Call as a separate component from Microsoft's prior initiatives due to its multi-stakeholder nature.

1.2 Research Question and Sub-Questions

In light of the introduction above, this thesis will seek to understand the role of the private sector in the field of diplomacy. Acknowledging the emerging diplomatic role of private actors in cyberspace, the question that will guide this research is:

Does Microsoft's engagement with diplomatic processes on (the stability) of cyberspace conform to the theoretical model of club diplomacy and/or are we witnessing a shift towards a model of network diplomacy in this area of international politics?

Guided by the main research question, the following sub-questions will be addressed:

(1) What is the state of the art in diplomatic theory on the (non)involvement of private actors in diplomatic processes and governance?

(2) What are the recent developments in the field of cyber diplomacy?

(3) How does Microsoft as an actor engage with the diplomatic processes

1.3 Academic Relevance and Societal Relevance

The academic contribution of this research provides an evaluation of which theoretical model best explains the recent developments in the field of cybersecurity. Additionally, the thesis will study how the field of cybersecurity can benefit from a multi-stakeholder approach as well as from the theory of global governance. The former appeals to the involvement of traditional public authorities and international agreements and at the same time underscores the need for private parties to enact these agreements (DeNardis 2017,13). The latter is based on a non-hierarchical culture that does not strictly refer to sovereignty rules and involves a multiplicity of actors which distinguishes it from the traditional theory of diplomacy (Cooper 2013, 44). To put it differently,

the 'new diplomacy' could use these approaches as an enhanced tool to effectively grasp the current advances in the field of cybersecurity.

Apart from academic relevance, this research also underpins the societal relevance of the shared management of cyberspace. This thesis will contribute to a better understanding of the benefits of multi-stakeholder governance of cyberspace. This is done through the evaluation of existing proposals in the field of cybersecurity namely the Paris Call for Trust and Security in Cyberspace and the Digital Geneva Convention. Both of these initiatives strongly emphasize the need of the involvement of all relevant actors (i.e. the civil society, the governments and the private sector) within the management of cyberspace, further underpinning the advantages of shared governance. More precisely, the Paris Call for Trust and Security of Cyberspace directly establishes the provisions of such cooperation which underpins the multi-stakeholder nature of cybersecurity and the need for a shared commitment to the protection of cyberspace (France Diplomatie 2019; Matsakis 2018). In the end, the thesis studies how the compromise of priorities between states, corporations and civil society provides a possibility that benefits all of the involved actors.

1.4 Reading guide

The introduction above has explained the focus and relevance of this thesis. Following, the structure of the paper will follow a logical development to answer the research question and sub-questions. The next chapter will present the theoretical framework within which this thesis is situated. Concepts of diplomacy, norm-entrepreneurship, (global) governance, as well as multi-stakeholderism, will be discussed as they provide the foundation for the research. As a consequence, the study of diplomacy and the diplomatic theory will be put into the context of current diplomatic practice in the field of cybersecurity. Afterward, chapter three will focus on the methodological underpinnings and the overall process of this research. The next chapter will provide an analysis of the results, where the research findings will be presented. This chapter will primarily focus on the engagement of Microsoft in diplomatic processes within cybersecurity. Additionally, the case will highlight the initiatives of the Digital Geneva Convention, and the Paris Call for Trust and Security in Cyberspace whose activity will be analysed through a content analysis complemented by media analysis. Finally, chapter five will link the findings to each other, followed by a conclusion which will complete the research.

2. Theoretical Framework

This chapter will focus on the academic debate regarding the participation of non-state actors in norm and rule setting, with a specific focus on the field of cybersecurity. The debate will be approached from three standpoints. First, the perspective of traditional diplomatic theory in regards to law-making will be addressed to establish the state of the art in the diplomatic theory on the (non)involvement of private actors in diplomatic processes. Second, norm-entrepreneurship will be introduced as a process that is distinct from the traditional diplomatic practice, in order to illustrate the role of private actors within this domain. Lastly, the multi-stakeholder governance model, which emphasizes the role of private actors in dialogues, decision-making and implementation of policies to shared problems, will be presented. By elaborating on these three perspectives, the theoretical framework will scrutinize the existing debate on the role of private actors in the field of cybersecurity and the recent developments in the field of cyber diplomacy.

2.1 Diplomatic Theory and Practice:

The roots of diplomacy can be traced back to 2500BC, the period when urban civilization emerged and commenced the exchange of diplomatic messages and treaties by royal envoys (Cohen 2018, 22). However, since then the diplomatic practice took many shapes and went through several processes of development. The traditional diplomacy as we know it began to evolve with the peace of Westphalia in 1648 which ended the Thirty Years' War and marked the development of an international system of sovereign nation states (Ibid., 33). The relations between the individual European States became so closely tied that the codification and consolidation of international law became essential for the peaceful management of international affairs (Ibid.) But it was only the Congress of Vienna in 1815, which marked the defeat of Napoleon, that commenced the series of peaceful negotiations among states as an established practice in the international legal order, also known as the Concert of Europe (Ibid.). Agreements and treaties between individual nation-states were recognized as binding, where consent became the touchstone of validity and rule of recognition (Farer 2013, 495). In this context, the right of sovereign states to form, interpret and implement law became the accepted status quo.

The foundations of the traditional diplomatic theory can be found in the Vienna Convention on Diplomatic Relations (1961) and the Vienna Convention on Consular Relations (1963) which establish the guiding rules of diplomatic practice (Cooper, Heine and Thakur 2013, 5). These conventions codified the rules of diplomatic practice with the main advance being the introduction of international conference for delegations to negotiate (Cohen 2018,34). This development marked the establishment of multilateral forms of diplomacy. Additionally, with regards to the diplomatic theory, these documents remain the core agreements which set the practical understandings of the diplomatic practice; they entail claims on what can be regarded as diplomacy in international relations, with focus on the specific traits and privileges of diplomats; and identify aspects important in international relations to enable a smooth process of the diplomatic system (Sharp 2018, 66).

Establishing the context of the traditional conduct of diplomacy, the 21st century debates about diplomacy focus at whether the sovereign as a centre of diplomacy is declining or adapting to the growing number of actors in the international arena. Since the 1980s the process of globalization has brought new political issues to the surface, such as humanitarian conflicts, economic stability and climate change, which increasingly involve a number of non-state actors in the matters of international relations. In this respect, these new power relations between the traditional state and non-state actors give rise to new practices of diplomacy. As a consequence, competing academic claims about the nature of diplomacy have been put forward.

According to Kerr and Wiseman, the practice of diplomacy is dominated by three claims: first, diplomacy is a state-based institution of professional and accredited diplomats whose legitimacy stems from the Vienna Conventions; second, another perspective maintains that diplomacy is partly a state-based institution which is part of a broader diplomatic system involving a plurality of actors; and finally, diplomacy is not the exclusivity of a sovereign, it is gradually becoming less so (Kerr and Wiseman 2018, 7). In this regard, it is accurate to think that there are being ‘diplomacies’ rather than a singular notion of diplomacy. Despite this plurality of opinions, diplomacy still remains a distinct feature of international relations, concentrated on communication, representation and negotiation of international relations (Ibid., 8). In order to understand the recent developments in the field of diplomacy, scholars identify two competing models of diplomacy, namely the club and network diplomacy, which best portray the changing nature of diplomacy.

Regulation of Cybersecurity: Power of Private Companies

Club diplomacy refers to a small number of players organized in a hierarchical structure in which the deliberation takes place behind closed doors (Cooper, Heine and Thakur 2013, 22). It is important here to mention that the traditional diplomatic practice is identified as a form of 'club diplomacy' which dominates the diplomatic theory. In this model, diplomats only meet with government officials and among themselves and do not really interact with business companies or civil society (Heine 2013, 60). Diplomats only negotiate agreements with each other, a practice that is deemed the most appropriate according to the views of club diplomacy. In other words, agreements are negotiated only between sovereign states. In the last decade, there has been a growing pressure on state diplomats to adjust to the new composition of global actors, since the non-state actors, specifically NGOs, are constantly creating and modifying the international and domestic institutions (Kerr and Wiseman 2018, 2). Upon these statements, Heine argues that state actors should engage in the practices of network diplomacy.

Network diplomacy is the reflection of the democratization process and the power of online media which increased the demand for greater transparency. This perspective stands in opposition to the traditional view of diplomacy where the main focus is given to the representatives of the states whose main role is to be the communicators of the nation who display their diplomatic relations to the public (Melissen 2005,5). In this context, the notion of network diplomacy highlights the myriad of actors at play in international interaction which rely less on administration and regulation, hence encouraging coordination of a vast network of actors (Heine 2013, 58). In this respect, sovereignty becomes less important than power outcomes. Therefore, Cooper, Heine and Thakur argue that the shift from club to network diplomacy is necessary in order to manage the interests of international players (Cooper, Heine and Thakur 2013, 22).

Kerr and Wisemann further appeal to polylateralism, the management of relations between state and non-state actors (Kerr and Wiseman 2018, 7). More precisely, diplomacy as traditionally perceived involves the communication of primarily state actors with other state actors, however this process has shifted over the years towards the inclusion of corporations and non-governmental organizations (NGOs) whose role is increasingly needed on the international stage (Melissen 2005, 11.). International companies have now similar interests with the states, that is assuring their accountability to the customers; being bounded by ethical and social responsibilities; and possessing a direct influence over the well-being of states. Non-state

organizations want to secure their place among key players by pursuing their objectives while challenging the role of the nation-state at the same time. In other words, diplomacy is perceived to be operating in a network environment where private businesses and non-state actors are regarded as diplomatic agents (Ibid., 12).

The current dynamics of diplomacy, involving the above-examined shift between the club and network diplomacy are best captured by the post-positivist school of thought. The growing belief among theorists of diplomacy (i.e. Sharp, Wiseman and Hall) asserts that the proportion of international relations conducted by accredited diplomats relative to all international relations is reducing given all the new actors on the global scene. The post-positivist school of thought lessens the assumption that diplomacy can only be conducted between states and that diplomacy needs to be precisely defined (Sharp 2018, 67; 69). Theorists of post-positivist school understand diplomatic practice as a fluid process in which diplomacy continuously adapts to the composition of the global order as well as to new forms of participation.

Considering the ideas of the post-positivist thought, such reasoning enables us to understand the dynamics of the current practice of diplomacy. Cooper, Heine and Thakur state that diplomacy today takes place among multiple sites of authority (NGOs, religious organizations, private companies, etc.). They further assert that adoption of policies is the responsibility of state actors, but the negotiation processes in many cases involve the participation of non-state actors and international organizations which are the main site of multilateral diplomacy (Cooper, Heine and Thakur 2013, 2). Despite these new transformations, states are and continue to be the only legal entities who hold the upper hand over the international order, with the ability to form, interpret and apply international rules and laws (Mačák 2017, 878; Cohen 2018, 36) Overall, states are the basic and enduring entity in international relations, however they need to adjust to the current diplomatic practice as the field of international relations is increasingly involving new actors and new forms of participation (Sharp 2018, 66.).

2.2 Norm-entrepreneurship

As mentioned above, there is an increasing role of non-state actors, mostly of NGOs, as policy shapers. The common roles of the civil society and the private sector in research, lobbying, advocacy and providing service are being extended to include functions such as the design and formulation of policies, providing non-state actors with the title of paradiplomats (Cooper, Heine

and Thakur 2013, 19). Additionally, non-state actors engage in activities which are in some instances limited to states, as they are often bounded by international conventions (e.g. in certain crisis situations NGOs are the only witnesses and therefore act as agents who perform functions usually carried by the state) (Badie 2018, 101). States depend upon these actors who in some cases are considered better informed and more legitimate. Nevertheless, despite the increasing inclusion of non-state actors in international institutions, many NGOs express frustration, claiming that even if they have a place to represent themselves and speak, they are not being heard. In other words, the new actors are being limited by the state's hierarchical and still dominant position in international relations.

When it comes to multinational corporations (MNCs), these are severely disenfranchised in decision-making bodies. Although MNCs regularly deploy agents to deliberate and negotiate directly with foreign governments to obtain concessions or to modify laws, they are being disregarded from any policy-making initiative (Cooper, Heine and Thakur 2013, 12). In general, states do not welcome new actors as they would undermine their dominant position, and as a consequence states create new ways which ultimately restrain new social actors in their actions (Badie 2018, 91). In the end, such practice underestimates these new actors and ignores their key role on the international stage.

Even though representation and communication, the main traits of diplomacy, are both performed by the private sector who wishes to remain legitimate in the eyes of their stakeholders and constituencies, it does not possess the sources of legitimacy that are desired by diplomacy (Pigman 2013, 194). According to Rudder, Fritschler and Choi, private governance is an overlooked area since most of the private operations lack transparency and are conducted within private companies in contrast to those of governmental institutions (Rudder, Fritschler and Choi 2016, 10). Therefore, the private sector takes on aspects of diplomatic actorness in its own right, given their need to represent themselves to other diplomatic actors as subjects of communication and representation (Pigman 2018, 79).

Against this background, private actors came to gradually assume the role of norm-entrepreneurs. This role is specifically relevant for the field of cybersecurity where the activity of private actors has become negatively affected by state-sponsored cyber operations. In this context, Deitelhoff and Wolf look at the way corporations get involved in the norm-making process. Enabled by the process of globalization, corporations propose and establish norms,

which continuously develop through ongoing processes where new actors extend or amend their meaning. Corporations have come to gradually shift their roles from norm-violators to norm-entrepreneurs in specific domains of public life given the decreasing capacities of the governments and the increasing role of the business sector in the world market (Deitelhoff and Wolf 2013,222). The spread of company codes of conduct, according to Deitelhoff and Wolf displays that we might be on the edge of experiencing a norm cascade within the private community with the private sector challenging the government as a norm-violating target. By proposing norms, companies set "a standard of appropriate behavior for actors with a given identity" (Finnemore and Sikkink 1998, 891).

Through the application of the original spiral model of human rights on the business sector, Deitelhoff and Wolf conclude that activities of private businesses have far-reaching effects on the legitimacy building of the private sector. The original spiral model assumes that the existence of a confrontational relationship between the government as a norm-violator and a transnational human rights network (i.e. NGO) will result in the norm-adjustment based on the strategies of naming and shaming. These tactics create a transnational structure capable of pressuring the norm-violating government (Deitelhoff and Wolf 2013, 225-226). In other words, companies level the playing field by proactively engaging in norm-setting in order to minimize the losses and bring the norm-violators into the question (Gorwa and Peez 2018, 9). This specifically applies to the case of cybersecurity where states are more often than not engaged in cyber attacks that negatively affect the businesses of the private sector, namely the technological industry.

Non-state driven initiatives provide a necessary intermediate stage towards a binding regulatory framework, offering experiment processes and modification practices (Finnemore and Sikkink 1998, 892). Moreover, these initiatives provide information to cover the technological knowledge gaps allowing states to consider the pros and cons of different proposals to decide which one is best to endorse. It is however important to remain that ultimately only states make international law. Besides, there are remaining questions about the potential legitimacy of the initiatives proposed by private actors (Mačák 2019, 85). In other words, non-state initiatives may be considered as norm-making laboratories for states' further activity in cybersecurity.

Such incentives can already be observed in the case of companies such as Microsoft and Siemens, as well as multilateral organizations such as NATO and OSCE (Organization for

Security and Cooperation in Europe) which took steps to defend the security of cyberspace. These initiatives come at a time when states are reluctant towards the development of legally binding rules which would regulate cyberspace since such laws would limit the anonymous activity of states in the online world (Mačák 2017, 887). The fundamental difference between the imposition of law and the imposition of a norm is that a violation of a legally binding law gives rise to international legal responsibility, whereas the same cannot be said of non-legal norms (Ibid., 882.). Since the establishment of laws guiding the cyberspace is at the moment far from reality, states resorted into the creation and imposition of norms guiding the behaviour in cyberspace (Ibid.). In that vein, legal uncertainty is useful for those with power to act in cyberspace to achieve their objectives.

Despite these advancements, norm-building initiatives still largely remain in the hands of state actors who fear that the new initiatives may challenge their dominant position. Furthermore, norm-setting initiatives by private sector are perceived with suspicion as these actors do not possess the sources of legitimacy that states do, which could eventually lead states to succumb to norms that would decrease their legitimacy (Badie 2018, 99). This is reflected in the fact, that so far private sector initiatives did not gain an official endorsement from any state (Hinck 2018). Instead, states continue to influence the global community through their own norm-setting initiatives, in the case of cybersecurity, the UNGGE.

2.3 Multi-stakeholder Model of Governance in Cyberspace:

Currently, private actors assume their role in the field of cybersecurity through the multi-stakeholder model of governance. In the case of cybersecurity, private actors are a part of the Internet Governance Forum which is a global multi-stakeholder platform that facilitates debates on public policy issues pertaining to the Internet (Internet Governance Forum-IGF 2019). Through this platform, various stakeholder groups, whether government representatives, civil society or private actors, interact in discussions related to the Internet on an equal basis. However, the forum does not offer any negotiated outcome, it only informs and advises those with policy-making power in the public and private sector (Ibid.). In this sense, the IGF does not provide private actors with the power to directly influence state behaviour in cyberspace but it provides them with a platform through which such initiatives can originate with the support of state actors.

Regulation of Cybersecurity: Power of Private Companies

The multi-stakeholder approach towards the governance of cyberspace is emphasized by the theory of global governance which highlights the advantages of cooperation between public and private entities. According to Levy and Kaplan, the role of the private sector in the field of global governance has de facto become a part of the fabric of the governance practice, as states have come to increasingly outsource private companies for the purposes of civil security (Levy and Kaplan 2008, 433). According to William Walters, governance implies the shift from institutions to processes of rule which take place beyond the affairs of the nation-state (Walters 2004, 29). Given the interconnected nature of today's society and the emergence of ever more complex networks, it appears that the political authority has become polycentric and multileveled (Ibid., 27). This conception of governance displaces the sovereign from its traditional role of securing order since new private regimes- i.e. complexes of formal and informal institutions- appear as a source of economic, social and political issue areas for wider international cooperation (Levy and Kaplan 2008, 441).

There is an active role of private actors in today's society which is indispensable in managing the increasingly complex environments of the international community. As Hocking points out, the policy network is formed through a set of relationships of different actors, which are non-hierarchical but at the same time interdependent with the main objective being the achievement of common goals (Hocking 2005, 37). These processes focus on governing mechanisms which do not arise from the governmental authority while being fluid, complex, dynamic and responding to changing circumstances (Walters 2004, 29.). Similarly, Levy and Kaplan argue that "the term 'global governance' refers to the emerging multi-layered and multi-actor system of global authority", where it does not only include national level regulation and formal international treaties but also private instruments such as codes of conduct and market structures (Levy and Kaplan 2008, 437). In this vein, this broader transfer of governance functions into the corporate sector plays a key role in shaping various aspects of society, ultimately recognizing the private sector as the protector of civil and political rights under the veil of corporate citizenship (Ibid., 434).

Expanding the notion of governance, DeNardis addresses the field of Internet governance and the role of power within the online environment. The author puts emphasis on the need of distributed governance arguing that: "The very definition of Internet governance is that it is distributed and networked multi-stakeholder governance, involving traditional public authorities

and international agreements, new institutions, and information governance functions enacted via private ordering and arrangements of technical architecture" (DeNardis 2017, 23). This shift towards multi-stakeholderism is further reinforced by Carr who advocates for the global provision of Internet governance and the specific roles of the involved actors. Carr states that the multi-stakeholder model is the best approach towards the governance of the Internet where multi-stakeholderism has become synonymous with global Internet governance (Carr 2015, 641). To put it differently, multi-stakeholder governance of the Internet is not only proposed as desirable but also essential for the effective governance of cyberspace where actors share responsibilities and stakes in the prospect of safe cyberspace.

Furthermore, states are now capable of exploiting critical information without being recognized which to a large extent hampers the conduct of private business operations. Given this limited statehood of cyberspace, governments began buying vulnerabilities- that are weaknesses or flaws of a private entity and vulnerability data about private services- to exploit sensitive data with the aim to pursue national objectives (Neutze and Nicholas 2013, 3). Since the majority of the networks is in the hands of private companies, the development of cybersecurity norms needs to involve the private sector as it presents the primary designer of the global ICT technologies and services (Ibid., 2). What role should the private sector have in cybersecurity, and how can such role co-exist with the traditional responsibilities of the state? The need for multi-stakeholder governance in the field of cybersecurity becomes essential and further explains how private actors, like Microsoft, enter the diplomatic field. Overall, even though multi-stakeholder governance is encouraged, neither states nor corporations have yet come to terms with their multiple roles in cyberspace. To overcome this roles'-expectations gap among the key actors, Microsoft has been at the forefront to establish a compromise between the stakeholders. The company is progressively asserting itself as a diplomatic actor through various processes which will be the focus of the following sections.

In conclusion, corporations and other non-state actors have grown to play a key role in the governance of cybersecurity. States, however, remain the chief regulators in their jurisdiction and in international institutions, hence possessing the power over the decisions made by non-state players. Concerning the first sub-question, according to the traditional diplomatic theory (club diplomacy), only states can form and apply international laws, a practice that will remain unchanged. However, a number of scholars argues that diplomacy needs to adjust to new

emerging trends as well as to the new composition of actors on the global scene (network diplomacy). Put differently, the broad transfer of state functions into the private hands establishes private actors as a part of the complex policy network that involves both state and non-state actors, whereby corporate and state leaders need to remain legitimate in the eyes of their stakeholders and constituencies

With regards to the field of cybersecurity, the growing number of state-initiated cyber operations has led private companies to engage in norm-developing initiatives through which they could influence states' behaviour in cyberspace. Despite the relevant reasons behind the involvement of private actors in norm-setting incentives, states are reluctant to express endorsement towards these initiatives as they do not perceive them as legitimate as state-led norm-building efforts. Yet, the arguments presented above demonstrated that private corporations should be perceived as legitimate players in the field of cybersecurity, with their role changing from that of norm-violator to norm-entrepreneurs.

The multi-stakeholder governance model offers private agents at the moment the best possibility to engage in debates related to the safety of the Internet. Being on equal footing with states and other civil actors, companies are able to advise policy-makers on issues regarding the regulation of cyberspace. Through these platforms private actors are able to cooperate with governments and develop proposals that can result in norm-setting initiatives. There is however an initiative that deviates from this understanding. The Paris Call for Trust and Security in Cyberspace is a proposal which is of multi-stakeholder nature, drafted in cooperation with Microsoft, announced at the UNESCO Internet Governance Forum, and at the same time endorsed by over 60 governments (Matsakis 2018). By being supported by as many governments, the Call is moving away from the multi-stakeholder arena towards the norm-entrepreneurship field, a shift that is contested by the diplomatic theory. The Paris Call and Microsoft's involvement in this context provide the foundation of this research.

The following analysis will study which model of diplomacy explains the best current practices in the field of cybersecurity based on the case of Microsoft and namely the initiatives of the Digital Geneva Convention and the Paris Call for Trust and Security in Cyberspace. In this respect, the following chapters will thus elaborate on these proposed question: How does Microsoft as an actor engage with the diplomatic processes? To understand the full complexity of

the matter, the thesis will elaborate in detail on both, the Paris Call and the DGC, which will provide the research with in-depth analysis as well as it will offer a base for further research.

3. Methodology

The theoretical framework above problematizes the conventional theory of diplomacy. While the traditional diplomatic theory does not involve any other actor than the state, in practice the coexistence and cooperation of various actors is increasingly visible in international affairs. Particularly, when it comes to the management of cybersecurity, the necessity of the private sector is clear, a development that is displayed through the initiatives of private companies who wish to propose norms regulating states' behavior in cyberspace. In this respect, the paper will closely look at the activity of Microsoft within the field of cybersecurity.

This section will focus on the methodological underpinnings, thus, the type of method for data collection, data gathering, operationalization of concepts, and lastly quality and inter-subject comprehensibility of the research.

3.1 Research Design

This research will follow a deductive approach including an exploratory case study design in order to answer the main research question. The case studies allow for the exploration and an in-depth understanding of complex matters, especially when a detailed analysis of a phenomenon is necessary. Specifically, the chosen design allows to provide a more in-depth idea of how the cases of Digital Geneva Convention and Paris Call are designed, and how these designs contribute to a greater success of one over the other. Furthermore, a case study provides a deeper insight on the ongoing processes and allows for a more rigorous analysis of specific developments (Lijphart 1971, 691). The method of exploratory case study design is usually applied as a step of explanatory research design, exploring relatively new fields of scientific investigation (Streb 2010, 2). The primary aim of the exploratory research is to observe the unknown, where the method benefits mostly from cases which "make the characteristic investigation field issues easily apparent" (Ibid.). In this context, the evident infiltration of the private sector into the diplomatic field provides a case to study given the fact that such phenomenon is contested in diplomatic theory. The choice of an exploratory case study research then, as a consequence, provides means for developing consecutive studies on a given matter, ultimately delivering a supportive role in developing continuative social research in general.

The paper will also examine proposed policy papers and documents drafted for both of

the initiatives (Digital Geneva Convention and the Paris Call) to observe the similarities and differences between the individual proposals, but also to understand the language used in each case for additional understanding of the aims of the proposals. In this respect, the content analysis in this research is seen as a halfway between the deductive and inductive approaches. Combining chosen methods of media and content analysis provides a mixed-method approach which delivers more robust and rigorous analysis of the cases. Given the timeframe of the research, the data gathering will be conducted over a six-week period to ensure the feasibility of this study.

3.2 Evaluation criteria

This thesis involves a qualitative content analysis for which evaluation research criteria must be developed that take into account its own goals, particular features and methodological starting points (Steinke 2004, 186). The primary aim of the paper is to explain how Microsoft as a corporate actor is involved in the diplomatic practice, therefore the main criterion was to evaluate initiatives which Microsoft is a part of. Secondly, through its activity, Microsoft has become the most politically active technology company. Since 2014, the company actively engages in promoting norms which would lead to safer environment of the Internet. The guiding document proposed by the company at the time was titled 'International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World', a paper which characterized the first comprehensive proposal of specific standards of behavior in cyberspace solely directed at the state's conduct in cyberspace (Mačák 2017, 888). This document was in 2016 revised in a form of a white paper termed 'From Articulation to Implementation: Enabling Process on Cybersecurity Norms' which proposed six cybersecurity norms regulating the state's behavior in cyberspace as well as six norms for the industry sector. Following that, the discussed initiative of Digital Geneva Convention was announced in 2017, calling for states to adopt cybersecurity norms which would ultimately lead to the establishment of a cybersecurity treaty. Given this extensive political activity of Microsoft and its clear ambition to appeal to national governments, the choice of Microsoft as the representative of the private sector for this research is appropriate.

Continuing, since the Paris Call for Trust and Security in Cyberspace is an initiative coming from the French government, this choice offers an insight on how a government-sponsored initiative is received compared to a one coming from the private sector. The French initiative was launched on November 12th 2018, producing a document titled 'Paris Call for Trust

and Security in Cyberspace' further establishing cooperative measures guiding the behavior of the civil society, the private sector and the state in cyberspace. With regards to this, the document was launched and drafted in cooperation with Microsoft and therefore for this reason the Paris Call provides a relevant case for further analysis (Matsakis 2018).

3.3 Data Analysis:

Qualitative Content analysis:

The documents chosen for content analysis are:

'*International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World'*- As mentioned above this paper was the first document that attempted at establishing norms which would guide the state behavior in cyberspace. It was later criticized by government representatives as it focuses too much on the state conduct and completely disregards the role of the industry sector (Mačák 2017, 888). Nevertheless, the document proposed six guiding norms which will be looked at.

'From Articulation to Implementation: Enabling Process on Cybersecurity Norms'- Following the initial proposal, Microsoft adjusted its stance and further established six more norms guiding the behavior of the industry sector complemented by the original six norms. In this way, the role of the industry sector in cyberspace shall be also guided by regulations, which will be focused at further in the paper.

Digital Geneva Convention White Paper- Finally, the Digital Geneva Convention which was announced in February 2017 called for the transformation of its six norms for state behavior in cyberspace into an international treaty. The document specifying the nature and purpose of the Digital Geneva Convention further proposed ten clauses on which states should rely while drafting such treaty.

'Paris Call for Trust and Security in Cyberspace'- The Paris Call aims to promote existing institutional measures with regards to the security of cyberspace. Furthermore, the document underscores a compromise of priorities between the state, civil society and the private sector. It sets out nine measures which strengthen the cooperation of the three actors. Since the document clearly argues for the participation of the private sector as well, it will be interesting to observe the extent of the measures and their applicability.

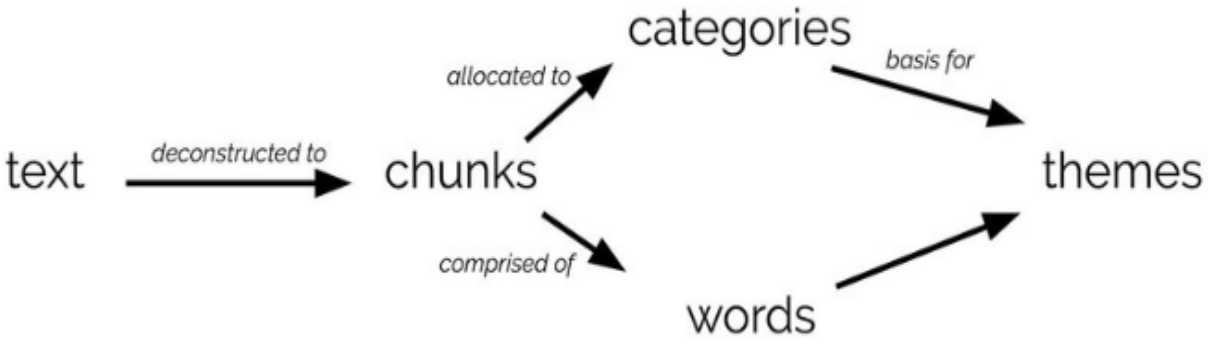
3.4 Operationalization of Data:

In what follows, a number of procedural techniques will be presented which will outline the operationalization of the data. First, a *summary of the content* was performed in order to reduce the material in a way that its essential parts are maintained for the analysis. Methods of omission, generalization, integration and bundling have been used to effectively reduce the studied material (Mayring 2004, 268).

Following the summary of the material, an *inductive category formation* is carried out. In this process, the summarization of the content provides a base for the development of emerging themes, which function as categories through which the answer to the main research question and sub-questions will be provided (Ibid.).

Third, the procedure of *explicating content analysis* aims to complement the summarized content with additional material. In this sense, this technique is the opposite of summarizing content, however is necessary to make collected textual pieces intelligible by adding further necessary information. For the purpose of this thesis, an additional media analysis will be conducted to complement the analysis of the above-outlined documents with supplementary explanatory material. Therefore, opinions and viewpoints of cybersecurity and diplomacy experts will be examined as well as reactions of state actors will be addressed. The main idea of this method is the systematic and controlled collection of complementary material, that makes it possible to "distinguish between a narrow contextual analysis that only involves the direct textual environment and a broad contextual analysis that collects additional material beyond the text" (Ibid., 268-269).

Finally, the *structuring of content analysis* is undertaken that seeks to filter out specific aspects of the material under stated criteria set prior to the conduct of the analysis. These have been developed in accordance with the theory (in this case the state of art in diplomatic theory on the (non)involvement of private actors in diplomatic and governance processes). The results will be outlined in the analysis section.



Mayring, Phillip. 2000."Qualitative Content Analysis Flow Chart." ***Forum: Qualitative Social Research*** **N.p.**

3.5 Quality of the Research and Inter-Subject Comprehensibility:

3.5.1 Quality of the Research

In order to ensure the quality of a qualitative research, criteria must be developed according to which the analysis can be performed. In the case of this qualitative research, terms 'validity' and 'reliability' are omitted for a specific reason. The concepts of validity and reliability have been originally developed for standardized quantitative research and are difficult to be transferred to a case of qualitative research (Steinke 2004, 186). This thesis will thus proceed with the following procedure.

Steinke identifies two core principles to ensure the quality of a research. First, a *conclusive discussion* of the quality of a research can be only conducted with reference to the corresponding research questions, methods, specific features of the research field and the object of investigation (Ibid.). Second, even though standardizability of procedures in qualitative research is restricted, the formulation of core criteria for a given research contributes to the overall quality of the research. In this sense, the formulation core criteria is central to the verification of the quality and orientation of the research (ibid.). In the case of this thesis, specific documents were chosen to answer the research question that correspond with the theoretical framework as well as contain all the necessary elements that need to be addressed within the analysis section. Finally, these criteria need to be defined in a way that that is specific to the investigation, that is, according to the research question and the identified problem within the academic debate (Ibid.).

3.5.2 Inter-Subject Comprehensibility

For qualitative research, unlike quantitative analysis, an identical replication of results is impossible due to the limited standardizability of methods within qualitative research (Ibid.). In this context, inter-subject comprehensibility of the research process provides a basis through which an evaluation of the results can take place. Through documentation of the research, this thesis will provide the foundations for inter-subject comprehensibility. In this way, the reader is offered the possibility to follow the progress of the analysis through which an evaluation of the research process and the results can be done (Ibid., 187). This is done to ensure the transparency of the study. Despite the fact that some level of subjectivity is unavoidable, the study will apply the above-identified techniques for content analysis which will limit the subjective involvement of the writer in order to improve the quality of the research.

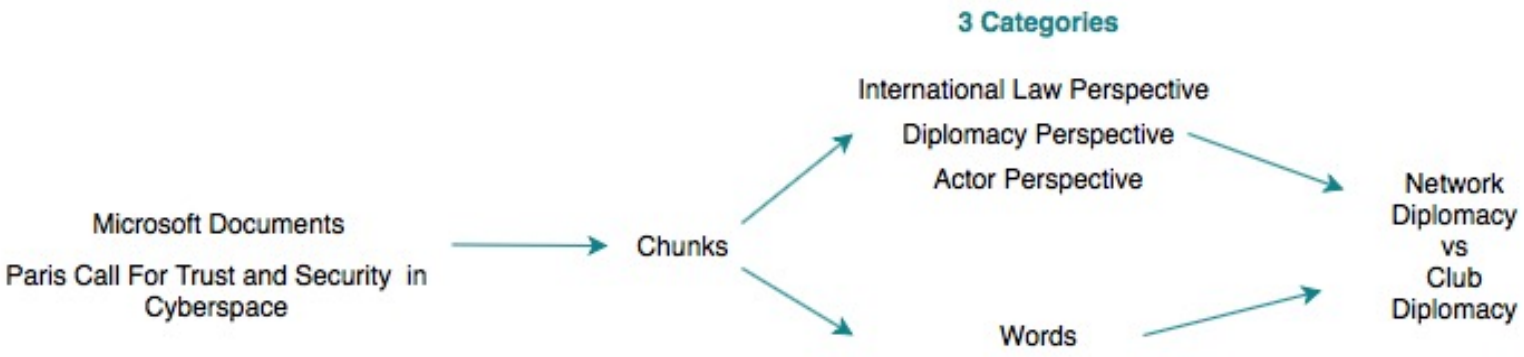


Fig. 1. Process of Qualitative Content Analysis Flow Chart

4. Analysis

In order to offer an analysis of the specified documents, the background on the work of Microsoft and the Paris Call needs to be addressed. In this respect, the thesis will look at what steps has Microsoft been taking in order to become a diplomatic player; how does the company influence the debate within cybersecurity; and what it aims to achieve with a multi-stakeholder approach. In this respect, the following question will be addressed: *How does Microsoft as an actor engage with the diplomatic processes?*

The paper will first address documents which have been drafted by Microsoft and after a separate section will be dedicated to the Paris Call initiative due to its multi-stakeholder nature. Afterwards, the thesis will explain the motives for both initiatives (i.e. DGC and Paris Call) followed by the analysis of the proposed documents. The content analysis focuses on the similarities and differences within the policy documents and helps to explain the reasons behind the success of the Paris Call compared to the failure of the Digital Geneva Convention. The content analysis is further supplemented by media analysis, followed by a review of Microsoft's engagement with diplomatic processes.

4.1 Microsoft's Engagement with Diplomatic Processes:

As explained above, Microsoft has attempted to assume its position as a diplomatic actor since 2014 by proposing whitepapers and policy documents. In this context the initiatives of Microsoft, namely the Digital Geneva Convention and the Cybersecurity Tech Accord may be perceived as a step towards an increased engagement in the cybersecurity norm-making processes through which Microsoft attempts to expand its boundaries of legitimacy (Hurel and Lobato 2018a, 10). This drive towards safe and transparent governance of the internet further emphasizes that governments need to evaluate their interests and priorities if they want to remain accountable to the public they represent.

By drawing on the theory of global governance and in broader terms referring back to the theoretical framework, Microsoft's case enables us to observe interesting findings on legitimacy building, norm-entrepreneurship, private governance as well as on the paradoxes of diplomatic theory in general. In this context, the theory of private governance can be directly applied to the case of Microsoft examining specifically corporate action. A corporate action is

understood as "an aggregate of complex associations between internal policy and technical teams, policy documents and initiatives, technologies and organizational infrastructures that support relations with governments and corporate customers" (Hurel and Lobato 2018b, 6). This approach is used as a tool of new private regimes through which Microsoft acquires its legitimacy within the private and public sector.

Microsoft's norm-building and rule-setting can be understood as a sequence of interactions on different levels. First, the technical development of software and technical tools to combat cybercrime takes place in the internal bodies of the company (Ibid., 2018b, 8). Second, the company attempts to establish cooperation among several companies which share the same interests in protecting cyberspace. And thirdly, Microsoft engages in norm promotion and active engagement with governments beyond national boundaries (Ibid.,9). In this way Microsoft builds its legitimacy through three dimensions: technological, among peers with other private companies and multi-stakeholder via engagement with governments.

Initiatives proposed by Microsoft offer an example of a company-led process directed towards the protection of cyberspace. Microsoft has sought to establish itself as the leader of the norm-making process, while at the same time attempting to establish itself as a diplomatic entity. After Microsoft's involvement in the NSA (U.S. National Security Agency) PRISM program, the activities of which led to the Edward Snowden revelations in 2013, the company started promoting norms that would lead to a safer environment on the Internet (Gorwa and Peez 2018, 10). In 2007 Microsoft became NSA's partner in their PRISM program, which collected Internet conversations from several US Internet platforms, providing the government with the ability to secretly access sensitive encrypted user data from various sources (Ibid.,8). Upon the 2013 Edward Snowden revelations, it was discovered that the activity of Microsoft along with two other big platforms, Yahoo and Google, comprised of 98% of PRISM's production (Gellman and Poitras 2013). After the Snowden leaks, NSA PRISM came to public attention, which negatively influenced Microsoft's user trust, resulting in Microsoft switching its position from being a willing collaborator in the PRISM program to actively promoting initiatives to make the Internet a safer space (Gorwa and Peez 2018, 8). Put differently, Microsoft needed to improve its reputation vis-à-vis its customers. In this respect, by establishing the Government Security Program, Microsoft demonstrated its determination to establish relationships with governments worldwide and to call for more transparency and trust-building.

The role of Microsoft as a cybersecurity norm-entrepreneur can be explored by following the spiral model of business sector analyzed by Deitelhoff and Wolf. After the NSA PRISM revelations, Microsoft became a big critic of the U.S. government's practices in cyberspace and progressively shifted its role from a norm-violator to a norm-entrepreneur. Rather than engaging in shaming tactics, the company proposed several initiatives, such as the Digital Geneva Convention, or the Cybersecurity Tech Accord through which Microsoft demonstrated its effort to protect cyberspace. The Cybersecurity Tech Accord is an initiative launched in 2018, that is built on a collaborative effort between technology companies and focuses particularly on improving the stability, safety and resilience of cyberspace (Cybersecurity Tech Accord 2019). In line with the spiral model, upon the increased vulnerability of the loss of reputation, Microsoft decided to become the promoter of the appropriate behavior in cyberspace.

To further substantiate these claims, it can be argued that contrary to the traditional corporate norm-entrepreneurship, the company engages in a multi-layered approach to cybersecurity. Microsoft does this through self-regulation and the use of the company's best practices that serve as norms for other companies. This is done in parallel with the promotion of initiatives at an international level through policy papers and recommendations for safe behavior in cyberspace (Hurel and Lobato 2018a, 8;10). Microsoft's initiatives and partnerships within the public sphere contribute to the company's authority, legitimacy and the growing perception of Microsoft as a diplomatic player. Through the use of semantics of international politics in its initiatives, Microsoft projects its voluntary self-commitment to the advancement of cybersecurity and its commitment to public expectations (Ibid., 7). This can be seen in the case of the Digital Geneva Convention and Microsoft's other initiatives.

4.1.1 Documents Proposed by Microsoft:

With regards to the activity of Microsoft, the company has over the years published three major documents focusing on responsible behavior in cyberspace. Beginning with their first document brought forward in 2014, the *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World* Microsoft aimed to establish six guiding norms for the behavior of nation states in cyberspace. The document, however, does not specify any norms to be adhered by the industry. Even though the text explores relevant roles for the private sector such as the coordination of vulnerability responses; exchange of Information; or the responsibility to respond

and recover from cyber attacks, it did not identify norms with which the private sector should comply. In this respect, the private sector appears to best operate as an actor which provides technical expertise for governments on a wide range of cybersecurity challenges, including the expertise on each of the norms proposed in the document (McKay et al. 2014, 16). Further, the document specifies that the private sector delivers in whole the critical information infrastructure and therefore the management of cyberspace must necessarily involve their participation (Ibid.). Therefore, the document appeals to the need for norms guiding the industry but does not propose any.

Following the first text, Microsoft released its second guiding document in 2016 titled *From Articulation to Implementation: Enabling progress on Cybersecurity Norms* which specifies six additional industry norms for the responsible behavior of the private sector in cyberspace. Building on its first proposal, Microsoft expresses its commitment to fulfill the expectations that customers have of the ICT industry. In this context, the document offers a collaborative approach between states and industries but also differentiates two important aspects between the two actors. Nation-states possess the ability to create mass effects through offensive cyber activities, while the global ICT industry has the ability to patch all customers, even during conflicts between and among governments (Charney et al. 2016, 6). Additionally, Microsoft recognizes the importance of the already existing initiatives focusing on the regulation of cyberspace and further specifies existing fora for the implementation of the proposed norms. Thus, the ultimate aim of this document was to emphasize the high level of collaborative and purposeful work necessary for the effective regulation of cyberspace.

Finally, the *Digital Geneva Convention* is an official policy paper produced by Microsoft in 2017 aimed at the establishment of norms for governments to protect cyberspace in peacetime and to prevent conflict. The ultimate goal of the proposal is the creation of a legally binding agreement that will ensure stable and secure cyberspace. With regards to this, the paper also states that there are already existing opportunities towards a legally binding agreement such as the Group of Twenty Countries (G20). What is of importance for Microsoft is the establishment of a legally binding framework rather than a prescribed approach towards this achievement (Microsoft 2017). The work of Digital Geneva Convention builds on existing proposals advocating for responsible state behavior in cyberspace. With its ten clauses the Convention aims to extend the scope of existing proposals and implement norms that Microsoft has proposed in its

past documents.

In order to understand the motives behind the Digital Geneva Convention, the analysis of the two preceding documents is vital. Microsoft's first two guiding documents have introduced six norms for responsible state behavior and six norms for the industry. The documents themselves, however, cannot be seen as policy papers as they are intended to be guiding documents putting forward a framework for developing cybersecurity norms. The first document introduces norms falling into two categories: norms improving defense and norms limiting offensive operations. The former is based on developing strong foundations for national cybersecurity capacities in order to reduce potential malicious cyber activities, while the latter focuses on ways to avoid escalation and limit any potential negative impact on the security of cyberspace.

As the initial white paper was criticized for its lack of norms which would target the activity of the industry in cyberspace, Microsoft released its second document which articulated six additional norms for industry behavior. Building on its first proposal, Microsoft added a third category of proposed norms, namely the industry norms. Furthermore, the document put forward an organizing model for developing cyber norms using a four-part framework of actors, objectives, actions and impacts which defines specific roles for the state and the industry within cybersecurity. Finally, it addressed the problem of implementation of norms within already existing fora focused on the security and stability of cyberspace.

Overall these documents provide a good background on the existing advancements and developments in cyberspace with further explanations of each norm that is being proposed. Additionally, it can be observed how Microsoft under the veil of corporate citizenship aims to protect not only its customers but also other industries from malicious cyber attacks. Given its technological expertise, but mainly the ability and responsibility to issue patches to protect ICT users, Microsoft levels the playing field by engaging in norm-setting in order to limit the effects of the state misconduct. Consequently, these texts paved the way for Microsoft to be perceived as an active player in the field of cybersecurity and thus strengthening its position within the debate.

Recognizing the effect of the proposed white papers, Microsoft continued to pursue its vision for a safe and secure cyberspace. The Digital Geneva Convention was supposed to do exactly that. Acknowledging the responsibility Microsoft has in safeguarding citizens around the world from state-led cyber attacks, the Convention aims to build on existing proposals within cybersecurity and paves the way for a legally binding agreement. The document addresses ten

guiding principles aimed at controlling state behavior in cyberspace.

Nevertheless, the document was perceived as flawed, mainly with regard to the language it chose to use. The main flaw of the document from the diplomatic perspectives is its title, namely the use of the concept of convention. Companies do not have the legitimacy to negotiate a convention, only states do, however it is not the objective of western countries to negotiate a new cyber convention (Lété and Chase 2018,8). If that would happen, the governance system within the field of cybersecurity would shift towards the preferences of Russia and China who wish to broaden the agenda to cover their proposals on 'information security' (Ibid.). This would mean the justification of domestic control over the use of the Internet, free speech as well as the right of the state to access user information.

Following, the word convention itself calls into question the application of the existing laws to cyberspace, consequently weakening the existing legal constructs captured in the work done by the UNGGE (Ibid.). Finally, the analogy made to Geneva indicates that Microsoft puts itself in the same position of the Red Cross, a three-time Nobel Prize Laureate who has the mandate to protect victims of international and internal armed conflicts (International Committee of the Red Cross 2019). In this context, Microsoft puts itself into an ambiguous position within the diplomatic sphere where it attempts to be recognized as an official diplomatic actor but falls short on the application of the diplomatic essence to its practice.

4.1.2 Paris Call for Trust and Security in Cyberspace:

Despite the criticisms expressed against the Convention, Microsoft has further advanced its position within the debate on cybersecurity and jointly drafted the Paris Call for Trust and Security in Cyberspace. French President Emmanuel Macron announced the Paris Call for Trust and Security in Cyberspace at the UNESCO headquarters in Paris on November 12, 2018, with the aim to protect the Internet against the threats and dangers existing in the digital space (France Diplomatie 2019). Prior to the announcement of the Paris Call, Microsoft has decided to establish its 'Digital Peace' campaign along with the Cybersecurity Tech Accord in early 2018 designed to offer better protection for its customers in cyberspace and security against cyber attacks. What is more, Microsoft first approached the French Government to obtain its support for the Cybersecurity Tech Accord, however France found the initiative to be too narrow and industry-oriented (Laudrain 2018). As a consequence, France saw the opportunity to take this problem into

its own hands and took the lead on governance in cyberspace, while closely cooperating with Microsoft on the design of the document. Through these constant actions towards the improvement of the safety of cyberspace, Microsoft asserts its place in the diplomatic arena. The Paris Call is a high-level declaration on developing common norms to limit hacking and destabilizing activities in cyberspace (Ibid.). Furthermore, the document is non-binding in its nature which means that it does not require governments or corporations to legally adhere to the proposed principles. Matsakis describes the initiative as a symbol of needed cooperation and diplomacy in cyberspace (Matsakis 2018). In that vein, the main ambition of the Paris Call is to gather and combine existing cyber norm proposals within a single document to create an effective framework for further discussions. In order to do so, the Paris Call had to first widen the scope of existing initiatives into meaningful norms that could be endorsed by the private sector, governments and the civil society. Second, it had to make sure that it collected and merged existing initiatives to avoid any fragmentation of norms (Laudrain, 2018.).

What is of importance is that the document was crafted in joint cooperation with Microsoft which demonstrates how tech corporations are playing a more active role in the governance of the Internet. Reacting to the initiative, Brad Smith stated that "It's an opportunity for people to come together around a few of the key principles: around protecting innocent civilians, around protecting elections, around protecting the availability of the Internet itself. It's an opportunity to advance that through a multi-stakeholder process" (quoted in Matsakis 2018). Additionally, Smith specified that the tech sector has the first and highest responsibility to protect digital technology and people who depend upon it, ultimately calling for the cooperation among governments, civil society and companies in the matters of cyberspace (Smith 2018). In this sense, the rhetoric of Brad Smith resembles one of a lawmaker which, in this case, should not come as surprising.

Acknowledging Microsoft's contributions, the Paris Call presents a policy that encompasses most of the existing cybersecurity initiatives. It reaffirms that international law, including the United Nations Charter as a whole, International Humanitarian Law and customary law is applicable to the regulation of cyberspace and thus endorses the work of the UNGGE. Furthermore, the document recognizes the work done and expressed within the Budapest Convention on Cybercrime and calls for the contribution of the private sector to ensure effective cooperation among all stakeholders. Finally, the Paris Call endorses the work of the Global

Commission on the Stability of Cyberspace (GCSC), namely the norms proposed in their Norm Package published in November 2018 as well as the *Call to Protect the Public Core of the Internet* which provides an elaborate definition of the public core (GCSC 2018). With respect to the language of the document, the presence of a state actor, in this case France, is clearly visible as the paper has the desired form, language and a structure of an official policy document which ultimately strengthens its value.

Regarding the success of the Paris Call, the initiative was endorsed by 64 governments, 328 private companies (i.e. Cisco, Facebook, Google, Siemens) and 129 universities, NGOs and professional associations (Laudrain 2018; Roy 2018, France Diplomatie 2019). In this way, the Call represents itself as the middle ground that represents the possibility to advance the progress towards safe cyberspace by including nation-states, private companies and the civil society. However, what is missing is the support of the major state actors, i.e. the United States, Russia and China whose inclusion is deemed vital for the regulation of cyberspace. This unwillingness of these actors can be attributed to the fact that their governments aim to keep an upper hand over the regulation of the Internet, pursuing their own initiatives and agendas. However, major American technology corporations like IBM, Corporation and Hewlett-Packard (HP), Google and Microsoft have expressed support for the deal which indicates the willingness of tech corporations to play an active role in the governance of Internet (Roy 2018). Despite these shortcomings, the Paris Call should be seen as a new means to achieve primary objectives of securing the cyberspace. Even though the document may be deemed imperfect, it arrives at a time when other governments have shown competing views on the control over cyberspace rather than seeking cooperation. In the meantime, the leaders of the Paris Call will pursue to gain the endorsement of the major countries, while America's largest companies will keep leading the way (Matsakis 2018). In the end, even though the support and signatures of these companies reflect that the Paris Call is here to stay, its success will be determined by the measures it decides to take in the foreseeable future. Overall, the Paris Call presents an option that at the moment offers the best of all, a favorable combination of existing norms.

In the end, the work of Microsoft can be divided into five consecutive stages: the development of norms for responsible state behavior; the development of industry norms; the Digital Geneva Convention; Cybersecurity Tech Accord; and finally, the Paris Call for Trust and Security in Cyberspace (Table 1 and 2.).

4.1.3 Summary of Proposed Norms:

Norms for Responsible State Behavior:
These norms focus and specify the behavior which states should exercise in cyberspace. The proposed norms recommend that:
(1) states should not target ICT companies;
(2) states should have a clear policy for handling vulnerabilities;
(3) the development of cyber weapons should be restrained and the use of such needs to be limited;
(4) states commit to non-proliferation of cyber weapons;
(5) states need to limit their engagement in cyber-offensive operations;
(6) states should assist the private sector in detecting and containing malicious cyber operations.

Industry Norms:
Industry norms are aimed at the responsible behavior of ICT companies in cyberspace and further advocate for the following norms:
(1) global ICT companies should not permit states to negatively affect their network;
(2) ICT companies should adhere to a clear policy on vulnerability handling;
(3) the ICT industry should not proactively defend against state attacks;
(4) global ICT companies should not traffic in vulnerabilities for offensive purposes;
(5) the ICT industry should assist the public sector in detecting and preventing events in cyberspace;
(6) the global ICT industry should issue necessary patches to protect ICT users.

Digital Geneva Convention:
The Digital Geneva Convention identifies ten key clauses for responsible state behavior. The attention is given to limited engagement of state actors in malicious cyber attacks and to the establishment of a clear policy for acquiring, retaining, securing, using, and reporting of vulnerabilities. Overall, the Digital Geneva Convention constitutes a blend of norms that have been advocated by Microsoft, with the main focus given on regulating state behavior in cyberspace.

Cybersecurity Tech Accord:
To protect the online environment, the Accord aims to adopt the following principles:
(1) to protect all Internet users and customers of the undersigned companies everywhere;
(2) to oppose cyber attacks on innocent citizens and corporations from anywhere;
(3) to strengthen cybersecurity cooperation;
(4) to partner with each other to enhance cybersecurity.

Table 1. Microsoft- Norm Development Process

Norms for Responsible State Behavior	Digital Geneva Convention
States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in products and services.	Refrain from attacking systems whose destruction would adversely impact the safety and security of private citizens (i.e. critical infrastructures, such as hospitals, electric companies).
States should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.	Refrain from attacking systems whose destruction could damage the global economy (e.g., integrity of financial transactions), or otherwise cause major global disruption (e.g., cloud-based services).
States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.	Refrain from hacking personal accounts or private data held by journalists and private citizens involved in electoral processes.
States should commit to nonproliferation activities related to cyber weapons.	Refrain from using information and communications technolog to steal the intellectual property of private companies, includin trade secrets or other confidential business information, to provide competitive advantage to other companies or commercial sectors.
States should limit their engagement in cyber offensive operations to avoid creating a mass event.	Refrain from inserting or requiring “backdoors” in mass-market commercial technology products.
States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.	Agree to a clear policy for acquiring, retaining, securing, using, and reporting of vulnerabilities in mass market products and services.
	Exercise restraint in developing cyber weapons and ensure that any that are developed are limited, precise, and not reusable.
	Agree to limit proliferation of cyber weapons. Governments should not distribute, or permit others to distribute, cyber weapons and should use intelligence, law enforcement, and financial sanctions tools against those who do.
	Limit engagement in cyber offensive operations to avoid creating mass damage to civilian infrastructure or facilities.
	Assist private sector efforts to detect, contain, respond, and recover in the face of cyber attacks.

Industry Norms	Cybersecurity Tech Accord
Global ICT companies should not permit or enable nation-states to adversely impact the security of commercial, mass-market ICT products and services.	We will protect all of our users and customers everywhere. -We will strive to protect all our users and customers from cyber attacks -We will design and deliver products and services that prioritize security and reduce the likelihood of vulnerabilities.
Global ICT companies should adhere to coordinated disclosure practices for handling of ICT product and service vulnerabilities.	We will oppose cyber attacks on innocent citizens and enterprises from anywhere. - We will protect against tampering with and exploitation of technology products and services during their development, design, distribution and use. -We will not help governments launch cyber attacks against innocent citizens and enterprises from anywhere.
Global ICT companies should collaborate to proactively defend against nation- state attacks and to remediate the impact of such attacks.	We will help empower users, customers and developers to strengthen cybersecurity protection. - We will provide our users, customers and the wider developer ecosystem with information and tools that enable them to understand current and future threats and protect themselves against them.
Global ICT companies should not traffic in cyber vulnerabilities for offensive purposes, nor should ICT companies embrace business models that involve proliferation of cyber vulnerabilities for offensive purposes.	We will partner with each other and with likeminded groups to enhance cybersecurity. -We will work with each other and will establish formal and informal partnerships to improve technical collaboration, coordinated vulnerability disclosure, and threat sharing.
Global ICT companies should assist public sector efforts to identify, prevent, detect, respond to, and recover from events in cyberspace.	
ICT companies should issue patches to protect ICT users, regardless of the attacker and their motives.	

Paris Call Cooperative Measures:

Contrary to the above-identified documents Microsoft, the text drafted by the Paris Call organizers combines and entails norms guiding the behavior of all actors dependent on cyberspace. It begins by acknowledging and welcoming the participation of private sector actors in improving trust and security in cyberspace. Then, it also promotes collaboration among

governments and civil society to create standards which enable a perfect framework for the regulation of cyberspace. Overall, the document calls for a multi-stakeholder approach to reduce risks to the stability of cyberspace and to increase the confidence and trust among the key players. Following the introductory statements, the paper introduces nine cooperative measures for the management of cyberspace (Table 2).

The measures proposed by the Paris Call focus primarily on the prevention of any activity that intentionally damages the core of the Internet including malicious cyber activities, intellectual theft, proliferation of cyber weapons and hacking. The document also focuses on strengthening norms promoting the security of digital processes, advanced cyber hygiene, and the need for a capacity-building in order to minimize malicious cyber activities. Lastly, the Paris Call also appeals to the implementation of confidence-building measures which would complement the norm-development process.

Table 2. Paris Call Cooperative Measures

Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.
Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet.
Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes through malicious cyber activities.
Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector.
Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm.
Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain.
Support efforts to strengthen an advanced cyber hygiene for all actors.
Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.
Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.

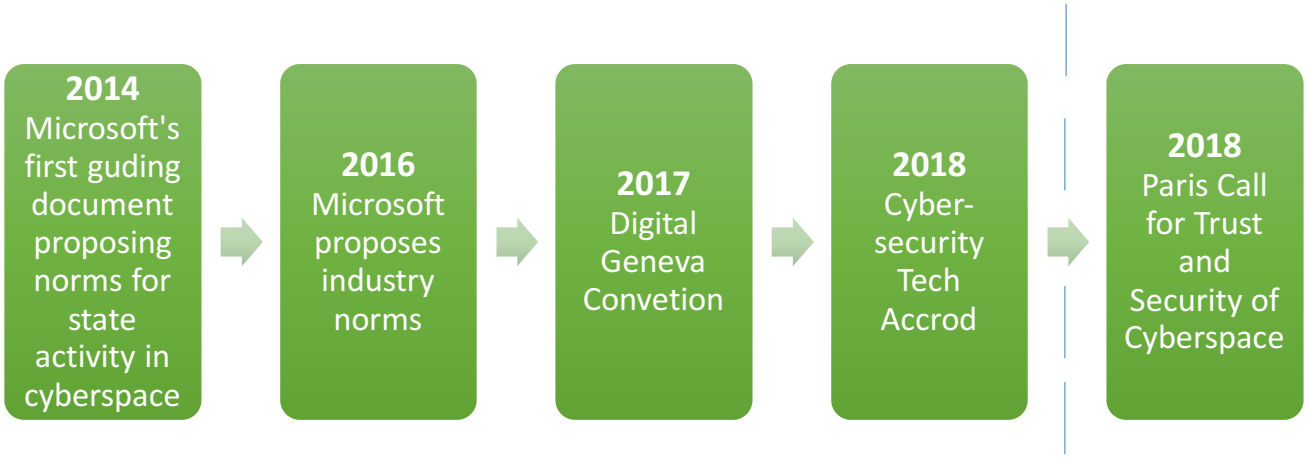


Fig. 2. Microsoft's engagement in norm-entrepreneurship in cyberspace

4.2 Reactions to the Digital Geneva Convention

Both proposals (i.e. DGC and Paris Call) generated a fair amount of reactions, perceptions and opinions on the engagement of Microsoft in the domain of cybersecurity. This section will analyse how different actors perceive each other namely how do they view and engage Microsoft in this domain. In order to address the full scope of Microsoft's engagement, the Digital Geneva Convention and Paris Call will be compared to each other in terms of their applicability.

Before elaborating on the reasons why the DGC is perceived as a failure from various perspectives, it is important to note that there is a shared agreement among cyber experts, academics and government representatives that initiatives such as the DGC emphasize the shared responsibility of governments and companies to keep cyberspace safe (Lété and Chase 2018, 4; Llorente 2018). Furthermore, the prominence that DGC has brought to the issue of shared responsibility underscores that the proposal fulfils a real need (Lété and Chase 2018, 4). Lastly, Microsoft employs humanitarian vocabulary and language similar to that used by civil society groups, thus appealing to the broader public and asserting its role in cyberspace (Llorente 2018). Ignoring the influence and expertise that Microsoft and other technology companies possess will only multiply the issues that cyberspace is currently facing.

In this vein it can be said that the DGC represents a new level of engagement that is unprecedented for a technology company (Ibid.). Microsoft is leading the charge in reshaping the international legal regulation of cybersecurity. By advocating for a Digital Geneva Convention Microsoft asserted itself as a moral actor looking for the greater good of society without fully

taking into account the importance of the concepts it utilizes. The Digital Geneva Convention, as attractive as it sounds, is a catchy name that can easily be distracted from its substance. In other words, despite the relevance of the idea behind the Convention, the language used within the proposal is perceived as a simplification of concepts for those working in the field of diplomacy and international law.

Regarding the reactions to the DGC expressed by experts in the field of diplomacy, cybersecurity and international law, it can be argued that the proposal is flawed from various perspectives. First, from the perspective of international law, DGC simply picks and chooses International Humanitarian Law principles and adjusts them at its convenience (Llorente 2018). More precisely, Microsoft proposes applying a convention that regulates war to peace time conditions. In other words, International Humanitarian Law applies in an armed conflict, while human rights law would be the applicable body of law in the context of DGC since it applies both in peace time and war time (Kilovaty 2019b, 20). The proposal, however, is unclear to which exact situations the Convention shall apply (Llorente 2018).

A consequence of this ambiguity towards the use of International Humanitarian Law is the assimilation of state-led cyber operations to armed conflicts by the DGC. In this context it should be stressed that International Humanitarian Law is already capable of regulating some aspects of cyber-warfare, however Microsoft's proposal applies this body of law to scenarios that are below the threshold of an armed attack (Casalini and Di Stefano 2018; Droege 2012, 533-534). Brad Smith envisioned the DGC to be the continuation of the original Geneva Conventions stressing that "just as the Fourth Geneva Convention recognized that the protection of civilians required the active involvement of the Red Cross, protection against nation-state cyber attacks requires the active assistance of technology companies" (Smith 2017). However, the ideological underpinnings of the Geneva Conventions are different from the ones behind the DGC. While the former aims to strike a balance between the protection of civilians and military defense in the context of armed conflict, the latter is driven by the need to strike this balance in peacetime conditions (Casalini and Di Stefano 2018). This fundamental difference between the two Conventions leads to a series of complications when applying the case of state-led cyber attacks to the military discourse.

Second, following the criticisms expressed by the experts in the field of law, the next paragraphs will analyze responses to the DGC put forward by diplomatic actors and states. One of the main objection towards the Convention argues that the proposal, if actually finalized, would replace the existing legal framework applicable to cyberspace that has been negotiated by the UNGGE. In this attempt the DGC challenges the success of the UNGGE, namely the consensus that international law applies to state behavior in cyberspace (Lété and Chase 2018, 8). According to a NATO report, "a Digital Geneva Convention could open opportunities to weaken existing statutes" ultimately calling for the establishment of a completely new international legal instrument (Ibid.). As a consequence, this would drive the governance system towards the preferences of Russia and China who essentially wish to implement domestic controls over the access to information.

In addition to NATO, Jacobsen published a comprehensive report that aims to represent the view of Denmark on Microsoft's proposal. According to Jacobsen, a proposal advocating for a convention is perceived as too ambitious, mainly because an initiation of a negotiation process is not necessarily desirable by nations, as guidelines on behavior in cyberspace to which states have agreed via the UNGGE process already exist (Jacobsen 2017, 5) Furthermore, drafting a new cyber convention would most probably lead to a failure as states are unwilling to give up on utilizing certain cyber tools, such as using IT vulnerabilities to catch criminals, reporting terrorist activities or conducting espionage (Ibid.) Moreover, the major state actors are unlikely to reach a consensus on a matter of a new cyber treaty due to their diverging perceptions about the regulation of cyberspace. Leading to the final point, a new negotiation process would cause the rise of diplomatic difficulties since reaching an agreement among 193 UN member states is much more daunting than continuing on the work already done in the field.

Jacobsen further argues that the Convention builds on the assumption that it is only states who are the main culprits in cyberspace. Even though state-led attacks do have severe consequences, companies that do not sufficiently comply with the fundamentals of IT hygiene are omitted from the proposal (Ibid., 15). Ultimately, the DGC, if formalized, would define the legal limits of state behavior in cyberspace, however it would not deal with the vulnerabilities developed by the technology sector. In this context, Microsoft should first engage in the evaluation of existing vulnerabilities in cyberspace, engage in and influence the ongoing negotiations on responsible state behavior, and ensure that the reached agreements are translated

into international practices. Second, following the criticisms expressed by the experts in the field of law, the next paragraphs will analyze responses to the DGC put forward by diplomatic actors and states. One of the main objection towards the Convention argues that the proposal, if actually finalized, would replace the existing legal framework applicable to cyberspace that has been negotiated by the UNGGE. In this attempt the DGC challenges the success of the UNGGE, namely the consensus that international law applies to state behavior in cyberspace (Lété and Chase 2018, 8). According to a NATO report, "a Digital Geneva Convention could open opportunities to weaken existing statutes" ultimately calling for the establishment of a completely new international legal instrument (Ibid.). As a consequence, this would drive the governance system towards the preferences of Russia and China who essentially wish to implement domestic controls over the access to information.

In addition to NATO, Jacobsen published a comprehensive report that aims to represent the view of Denmark on Microsoft's proposal. According to Jacobsen, a proposal advocating for a convention is perceived as too ambitious, mainly because an initiation of a negotiation process is not necessarily desirable by nations, as guidelines on behavior in cyberspace to which states have agreed via the UNGGE process already exist (Jacobsen 2017, 5) Furthermore, drafting a new cyber convention would most probably lead to a failure as states are unwilling to give up on utilizing certain cyber tools, such as using IT vulnerabilities to catch criminals, reporting terrorist activities or conducting espionage (Ibid.) Moreover, the major state actors are unlikely to reach a consensus on a matter of a new cyber treaty due their diverging perceptions about the regulation of cyberspace. Leading to the final point, a new negotiation process would cause the rise of diplomatic difficulties since reaching an agreement among 193 UN member states is much more daunting than continuing on the work already done in the field.

Jacobsen further argues that the Convention builds on the assumption that it is only states who are the main culprits in cyberspace. Even though state-led attacks do have severe consequences, companies that do not sufficiently comply with fundamentals of IT hygiene are omitted from the proposal (Ibid., 15). Ultimately, the DGC, if formalized, would define the legal limits of state behavior in cyberspace, however it would not deal with the vulnerabilities developed by the technology sector. In this context, Microsoft should first engage in the evaluation of existing vulnerabilities in cyberspace, engage in and influence the ongoing

negotiations on responsible state behavior, and ensure that the reached agreements are translated into international practices.

Finally, DGC calls for an attribution organization which would evaluate cyber attacks and identify perpetrators. In other words, it calls for the establishment of a Cyber Red Cross as a global institution to promote stability, security and trust in cyberspace. In this way, Smith creates an analogy to the International Committee of the Red Cross as he positions technology companies to be the Internet's first responders to a cyber attack, similarly as the Red Cross plays an active role in civilian protection in times of war (Smith 2017). This proposition has been criticized from two standpoints. First, to compare Microsoft to an institution which is neutral, not motivated by profit and governed by clear rules, norms and values, with the consent of state parties of the Geneva Conventions is not necessarily a view shared by nation states (Kilovaty 2019b, 22).

Second, the establishment of such organization would mean that technology companies would have the access to state (intelligence) services, thus possessing unprecedented power in the governance of cybersecurity (Kilovaty 2019b, 25; Jacobsen 2017,16). However, states are rarely willing to reveal the evidence they possess as it could act against the future collection of such information. Following, an attribution organization would constantly have to be at the forefront of cybersecurity knowledge and expertise, two elements that are specific to the technology sector (Kilovaty 2019b, 28). Furthermore, cyber agency, as envisioned by Brad Smith would also focus on preventive cybersecurity which involves the monitoring of vulnerabilities developed by the technology sector as well as the reduction of the likelihood of vulnerabilities (Jacobsen 2017, 16). In this context, access to certain services is thus necessary for private actors to effectively investigate cases of cyber attacks. Despite the great technical expertise of these companies and the prospects of an independent cyber agency, states are unlikely to grant such concessions to these actors.

In the end, the idea of a Digital Geneva Convention serves a good purpose in that it attempts to protect civilians against a real threat. However, it needs to be maintained that despite the influence and prominence of the Convention among stakeholders, governments and cybersecurity experts are aware that the name cannot be easily distracted from its substance. It is

up to governments and technology sector to debate on specific agreements which would be beneficial to all. The following section will examine reactions expressed towards the Paris Call for Trust and Security in Cyberspace.

4.3 Reactions to the Paris Call for Trust and Security in Cyberspace

Moving now onto the Paris Call for Trust and Security in Cyberspace, the initiative has received a great amount of attention as well as admiration. Compared to the DGC it can be argued that Paris Call is a success, essentially given to the fact that several governments have expressed their support, something the DGC failed to achieve. The support can be explained by examining the nature of the document.

To begin with, the Paris Call reaffirms the application of international law, including the Charter of the UN in the field of cybersecurity. It furthermore reaffirms the applicability of the international human rights law in cyberspace. These affirmations represent a clear distinction from the DGC, which is unclear about the type of law it wishes to enforce in its proposal, making it difficult to enforce the norms it recommends. In this context, the Paris Call acknowledges the work done by the UNGGE, recognizes the Budapest Convention on Cybercrime as well as it supports a norm package proposed by GCSC in late 2018.

Apart from expressing the support for the existing measures, the proposal states that International Humanitarian Law and customary law are applicable to the use of information and communication technologies by states (Moulin 2019). In contrast to the DGC, such a statement does not evoke ambiguity as the proposal is not specific on the fact in which situation it wishes to apply the cooperative measures it proposes. However, it needs to be stressed that the interpretation of the Law needs to take into account the specificities of cyberspace, a view expressed by the International Committee of the Red Cross, where in some instances new stricter rules may be necessary (Droege 2012, 534). What is missing from both proposals is the clarification of how and in which situations does the International Humanitarian Law apply to cyberspace as it constitutes a domain different from the one of military defense. So far international law seems to be unable to explain this matter which represents a significant gap within the existing legal framework that is difficult to solve (Kilovaty 2019b, 9). In order for any norms to be potentially adopted in the domain of cybersecurity a clear interpretation of international law is needed.

Continuing, an important innovation put forward by the Paris Call is the purposeful empowerment of the role of the private sector within cybersecurity. This recognition is visible through the cooperation with Microsoft who first approached the French government to obtain its support for the Cybersecurity Tech Accord. According to David Martinon, the French ambassador for Digital Affairs, it is essential to ensure the stability in cyberspace not only through negotiations with nation states but also through dialogues with private individuals, whether those are companies or the technical community (Martinon 2018). In this way France succeeded in attracting the support of the Tech Accord which represents a significant share of the private sector signatories. The empowerment of the private sector is further enhanced within the proposal: "In order to respect people's rights and protect them online as they do in the physical world, States must work together, but also collaborate with private-sector partners, the world of research and civil society" (France Diplomatie 2019).

The Paris Call also reflects the view of most states as it seeks to promote the exclusive role of sovereign states when it comes to conducting hostile acts in cyberspace. It adopts a straightforward approach to corporate hack-back and other offensive operations coming from the private sector. In order to further obtain the support from the state actors, President Macron suggested that the Internet Governance Forum should become responsible for the implementation of the Paris Call and should fall under the direct supervision of the U.N Secretary General (Laudrain 2018). Through this act Macron fully acknowledges the importance of the role of nation states, specifically the UN-led process in the field of cybersecurity.

According to all these views, the Paris Call seems like the perfect document to be followed. However, like any other initiative, the Call has some flaws that have been put forward by experts in the field of cybersecurity and non-state organizations. The main weakness of the proposal is the absence of support from major cybersecurity players, i.e. the United States, Russia and China. This is mainly due to the fact that these players want their own interests and agendas to be put forward. Following, the Paris Call did not establish any compliance mechanism which means that it does not require the signatories to legally adhere to the proposed norms (Moulin 2019). Nevertheless, it deserves recognition for relaunching the discussions regarding cyberspace one year after the UNGGE process reached an international deadlock.

Following, not all actors who support the Paris Call agree with all of its propositions.

Access Now, an international non-profit organization which advocates for free and open Internet, criticized some parts of the agreement as they lacked clarity and were insufficient. According to Drew Mitnick, policy counsel at Access Now, the promotion of 'cooperation' of stakeholders against cyber criminality does not fully reflect the relationship between law enforcement and companies (Mitnick 2018). He states "Cooperation, on the other hand, can be interpreted to mean informal exchange of data or the intentional weakening of platforms to enable law enforcement access" (Ibid.). In other words, this proposition could mean that companies and governments could share information and data without any judicial orders. Further, the Paris Call does not adequately address the risks of government hack-back, neither does it sufficiently specify the dangers of government hacking. In this sense, government hacking does not only entail major cyber attacks, but also espionage and invasive malware operations which are not addressed in the document. Such activity could pose a threat to user privacy as well as undermine the security of ICT platforms (Ibid.).

In the end, a general consensus on the importance of the Paris Call has been expressed by governments, businesses and the civil society. By advocating for the shared commitment of all stakeholders, the Paris Call at the same time limits the power of sovereignty, which is often used as a justification for data collection, government hacking and infringements on user privacy. Furthermore, it recognizes the role of the technology sector, namely the Cybersecurity Tech Accord, and goes one step further in implementing norms suitable for its signatories. As a consequence, the adoption of these norms provides incentives for technology companies to decline the delivery of cyber offensive capabilities to governmental clients (Lété and Chase 2018, 13). Finally, the Paris Call is a necessary step towards increasing Internet security and can be understood as an extension of governmental and non-governmental (i.e. UNGGE and Microsoft) cybersecurity initiatives aimed at reaching unified and effective Internet regulation (Moulin 2019).

4.4 Review of Microsoft's Engagement with Diplomatic Processes:

Based on the analysis of the two proposals it is clear that Microsoft undertook different paths to pursue its role in the domain of cybersecurity. Its activity can be summarized through three categories of evaluation that capture Microsoft's continual progress in engaging with diplomatic

processes. The categories are as follows: Microsoft has first asserted its democratic legitimacy in the field of cybersecurity by assuming the role of a norm-entrepreneur after the NSA revelations; second, Microsoft engaged in the establishment of initiatives independent from governments emphasizing neutrality and transparency; finally, Microsoft has partnered up with the French government and jointly drafted the Paris Call for Trust and Security in Cyberspace.

Regarding democratic legitimacy, technology companies usually do not possess the same sources of legitimacy in creating law and norms as state actors do. Nevertheless, Microsoft has gradually asserted its legitimacy within cyberspace following the NSA PRISM revelations. In order to restore its reputation and remain legitimate in the eyes of its clients and stakeholders, Microsoft shifted its role from that of norm-violator to a norm-entrepreneur. Microsoft's strategy of acquiring legitimacy consists of engaging in different dimensions of cybersecurity: technical, among technology companies and through multi-stakeholder negotiations. This engagement is seen through the initiatives of Cybersecurity Tech Accord which calls for the cooperation among the technology sector, the Digital Geneva Convention and the Paris Call for Trust and Security in Cyberspace, the latter being an initiative advocating for a multi-stakeholder approach towards cybersecurity. Microsoft's eagerness to become involved in the regulation of cyberspace has been noticed by both, state and non-state actors mainly through the DGC and has been further reinforced by its involvement in the Paris Call. By undertaking all these steps, Microsoft has asserted its legitimacy in cyberspace.

Following, Microsoft drafted and established several initiatives aimed at protecting and securing cyberspace through which the company asserts its neutral stance and promotes transparency. For an example, in its Cybersecurity Tech Accord Microsoft adopted a clear neutral stance stating "We will not help governments launch cyber attacks against innocent citizens and enterprises from anywhere" and "We will strive to protect all our users and customers from cyber attacks irrespective of their technical acumen, culture or location, or the motives of the attacker, whether criminal or geopolitical" (Cybersecurity Tech Accord 2019). To appeal to its international clients, the key actors in the growth and success of ICTs companies, Microsoft casts itself as "neutral amidst the competing claims by national governments and in the face of claims by the U.S. government for preferential treatment because of their status as a U.S. company" (Eichensehr 2018, 32). Furthermore, in its report NATO stresses that the Accord is a clear signal that the private sector is willing to engage and to adopt responsibility in cyberspace (Lété and

Chase 2018, 13). Governments should welcome this incentive by assisting the private sector to enlarge the group of companies that are part of the Accord and by promoting its values, eventually attracting non-western ICT businesses as well as from Russia and China.

> *Nation states can further play their part by working with industry on two other fronts. First, by stepping away from narrow national visions and working toward an internationally accepted definition of what industry responsibility means. And second, by encouraging national administrations to set up channels that allow industry to more effectively work with governments to fight the use or misuse of vulnerabilities in software systems and to limit the extent to which governments can covertly use these. (Ibid.)*

Furthermore, to complement the principle of neutrality, transparency is another feature specific to private actors. Transparency is one of the central values that Microsoft aims to embrace through which the gap between companies and clients can be reduced. Microsoft promotes this approach through its Government Security Program that provides its governmental clients with Transparency Centres. Through these centres "Participants have access to source code and an environment for in-depth inspection with advanced tools" (Microsoft 2019). More precisely, Transparency Centers offer governmental clients the opportunity to review information on cybersecurity threats and vulnerabilities directly benefiting from the expertise of Microsoft specialists.

Finally, by cooperating with the French government on the Paris Call, Microsoft fully demonstrated its will to take part in cyber diplomacy. It needs to be stressed here, that Microsoft is not on equal footing with nation states. Examining the number of constituencies Microsoft has, the company would be placed third on the ranking of countries by population (Eichensehr 2018, 20). In this context a policy change by Microsoft affects a bigger number of people than any governmental policy change, with the exceptions of India and China (Ibid., 21). In this sense the main source of power for Microsoft becomes its transnational influence arising from its non-territorial characteristic. For this reason, however, it needs to be maintained that technology companies exercise substantially less authority over their constituencies than territorial sovereigns. Even though some explanations may suggest that the influence technology sector possesses is similar to that of a state actor, companies do not enjoy having their own territory or sovereignty.

Regulation of Cybersecurity: Power of Private Companies

It is essential to emphasize that ICT companies lack the two main characteristics that would make them equal to state authority, namely territory and sovereignty. According to Max Weber, "state is a human community that (successfully) claims the monopoly of the legitimate use of physical force within a given territory" (quoted in Gerth and Mills 1946, 77). Microsoft lacks the prominent feature of territory and it is unlikely that it will develop one in the near future. Furthermore, sovereignty provides states with the right to assert their power whenever they feel that private platforms exert too much power (Kilovaty 2019b, 47). Microsoft nonetheless is a powerful actor within the field of cybersecurity and rightly so as the majority of the Internet structure is privately owned. While it is true that technology platforms do not have a monopoly over the use of force or a defined territory, their growing influence in the 21st century can be described as a new way of asserting authority which challenges the notion of power that is traditionally linked with states (Ibid.,48).

This new type of power has been termed as functional sovereignty which implies that a given private actor is no longer one of many market participants but instead is the leader and supervisor of these participants (Pasquale 2018,1). Pasquale argues that ICT companies are no longer merely market members, they exert regulatory control and become policy-makers in their fields (Ibid., 2). The ability of platforms to act as powerful gateways not only enables them to dominate the markets but also to displace a wide array of governmental roles from room lending to transportation (Froissart 2019). As a consequence, citizens are becoming subjects to corporate rules and regulations. The activity of Microsoft and other similar private actors then represents a shift from territorial sovereignty to functional sovereignty. This excessive power of digital giants carries risks in that companies can gradually assume monopolies in their fields that hinder the rise of potential competitors, but also limit choices for consumers. In order to curb this power, only governments can prevent functional sovereigns from taking over government-like roles. In this context, to ensure that citizens are protected and enjoy the advantages of digitalization, international cooperation and involvement of private actors are essential as digital platforms provide great benefits to consumers and societies (Pasquale 2018, 3; Froissart 2019). However, regulatory frameworks can only originate from state power, a prerogative that underlines the dominant role of states in law-making.

Conclusively, regarding the role of the private sector within cybersecurity, specifically within the UN, states have increasingly called for the active participation of the private sector in

discussions regarding the safety of cyberspace. This view has been expressed in resolutions put forward by both the Russian and American governments, and adopted by the General Assembly stressing that "while States have a primary responsibility for maintaining a secure and peaceful information and communications technology environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations" (United Nations General Assembly 2018). In this respect, states have come to recognize the contribution that private actors can have to the field of cybersecurity. However, there is yet no clear definition of the role of private parties within diplomatic institutions. In other words, the involvement of Microsoft and other private entities is acknowledged but the appropriate mechanisms for participation remain to be developed.

5. Conclusion

The conclusion below provides a detailed understanding of the analysis. It links the findings together to better understand the overall perspective of Microsoft's engagement in the field of cybersecurity and its engagement with diplomatic processes.

5.1 Conclusion

The analysis in this thesis illustrates how private actors, specifically Microsoft, have grown to become involved in norm-making processes, especially in the field of cybersecurity, and whether this involvement is successful. Overall, the study grows out of academic interest to observe whether Microsoft has the ability to shape politics within cyberspace and if so to what extent. That is, the study aimed to research whether Microsoft's engagement with diplomatic processes in cyberspace conforms to the theoretical model of a club or network diplomacy in the field of cybersecurity. To answer the main research question, this section will reflect on the sub-questions guiding this research.

The first and second sub-question, "*What is the state of the art in diplomatic theory on the (non)involvement of private actors in diplomatic processes and governance?"* and *"What are recent developments in the field of cyber diplomacy?"* were outlined in the theoretical framework. The paper demonstrated that according to the traditional diplomatic theory, nation states are the only actors in the area of international relations with the power to create, implement and modify laws. However, with the globalization process, new political issues were brought to the surface, consequently involving a number of non-state actors in matters regarding international relations. These emerging challenges gave rise to new practices of diplomacy that led to the establishment of new power relations between state and non-state actors.

In regards to the field of cybersecurity, two theoretical models of diplomacy that best portray the changing nature of cyber diplomacy were introduced, namely the club and network model of diplomacy. While the principles of the former are synonymous with the traditional diplomatic theory, the latter appeals to the cooperation among state and non-state actors to effectively manage current developments in cyber diplomacy. By examining recent developments within the field of cybersecurity, the thesis showed the prevalence of the network model of diplomacy when it comes to actor participation.

Regulation of Cybersecurity: Power of Private Companies

It was displayed that the involvement of private actors in matters regarding the regulation of cyberspace progressively grew, as the amount of state-led cyber operations increased over the last decade. As a consequence, ICT companies have become negatively affected by unregulated state behaviour, which led private actors to engage in norm-entrepreneurship. Even though states remain the only actors who have the power to establish and apply international laws, the area of norm-entrepreneurship is becoming more open to private actors, specifically within the field of cybersecurity. Despite the prominence of the state-led UNGGE process, states have themselves called for the active participation of the private sector in discussions regarding the safety of cyberspace. While the progress of the UNGGE cannot be denied, private actors have realized the severity of state-sponsored cyber attacks, resulting in the establishment of several norm-making initiatives parallel to the UNGGE process. As the last round of UNGGE failed to put forward a consensus report, these non-state initiatives gained more attention within the debate on the safe regulation of cyberspace.

The most prominent proposal aimed at the governance of cyberspace has been the Paris Call for Trust and Security in Cyberspace presented by the French government at the Internet Governance Forum in November 2018. The Call was drafted in joint cooperation with Microsoft which underpins its multi-stakeholder nature and the engagement of a private actor in diplomatic processes in the field of cybersecurity. What is more, the Paris Call has been endorsed by over 60 governments, a development which moves the initiative from the sphere of multi-stakeholder arena towards the norm-entrepreneurship field. Taken together, these emerging trends challenge the traditional perception of club diplomatic theory

Given the technical expertise of the private sector and its ability to issue patches to victims of cyber attacks, states have acknowledged the participation of private sector in the fabric of global governance by transferring some of their governance functions into the private sphere. As a consequence, the private sector is to a large extent involved in regular negotiations with governments in order to create the most satisfactory conditions for their peaceful coexistence. The paper demonstrated that this interaction among stakeholders is advanced by the principles of global governance which provides actors with a field of proliferating networks where different actors engage in managing them, thus creating a multi-actor and multi-layered system of global authority. Enabled by the practices of global governance, private actors engage in processes of cyber diplomacy through a multi-stakeholder governance approach and progressively assert their

role in norm-making initiatives. The thesis offered a case study of Microsoft through which this development was analysed.

The analysis in chapter 4, aimed to answer the third sub-question *"How does Microsoft as an actor engage with the diplomatic processes?"* Through a content analysis of documents put forward by Microsoft, the Paris Call for Trust and Security in Cyberspace, complemented by media analysis, this paper argues that Microsoft engages with diplomatic processes through a sequence of interactions at different levels. Microsoft has first assumed its democratic legitimacy within the field of cybersecurity after the NSA revelations, switching its position from a norm-violator to a norm-entrepreneur. Following, the company established various initiatives, such as the Cybersecurity Tech Accord, the Government Security Program and the Digital Geneva Convention, through which Microsoft demonstrated its intent of advancing neutrality and transparency in regulating cyberspace. Finally, through its cooperation with the French government, Microsoft has asserted its role in norm-entrepreneurship, an attainment that contests the traditional model of club diplomacy and conforms to the practices of the network model of diplomacy. The analysis depicted the reasons behind the success of the Paris Call compared to the failure of the Digital Geneva Convention through perceptions of international law, diplomacy and perspectives of other actors active in the field of cybersecurity.

In conclusion, through the analysis of the Digital Geneva Convention and the Paris Call for Trust and Security in Cyberspace, the research showed that Microsoft's engagement with diplomatic processes on the stability of cyberspace conforms to the network model of diplomacy. More precisely, through building its democratic legitimacy, establishing independent initiatives, and cooperating with the French government, Microsoft has entered the field of norm-entrepreneurship where its participation has been acknowledged by a number of governments. The thesis argues that Microsoft's case represents a shift from territorial sovereignty to functional sovereignty, whereby the transnational influence and resources that the company possesses enables it to dominate markets and thus displace an array of cyber-related governmental functions. In order to ensure the safety of cyberspace, governments and private actors need to establish regulatory frameworks that are universally beneficial. In sum, the effective regulation of cyberspace calls for multi-stakeholder cooperation among all actors through defined mechanisms of participation.

5.2 Limitations of the Research

Based on the findings of this research it can be said that the content analysis and the methodological approach within this thesis provided the necessary framework that allowed to display the perceptions on Microsoft's engagement with diplomatic processes. However, the limitation of this study concerns the generalizability of the findings as the paper focused only on one case, which is unique within the field of cybersecurity. Moreover, the research was limited only to content analysis and media coverage. Future research would benefit from a broader methodological approach, including interviews with experts in fields of cybersecurity and diplomacy that would add overall strength and value to the analysis. Further, an interesting study would contain a comparison of two companies involved in the regulation of cyberspace to analyse whether current developments in the field of cybersecurity conform to the theoretical model of network diplomacy.

Moreover, the analysis was conducted by the researcher herself and no guarantee can be given that the core and evaluation criteria employed were kept constant as the researcher bias constitutes an uncontrollable risk to the quality and inter-subject comprehensibility of the research. For future research it is recommended to employ interpretations in groups in order to ensure the inter-subject comprehensibility of the research. This entails a discussion of the research with multiple people who do not work on the same research. Consequently, a higher agreement among colleagues would indicate that they apply similar core and evaluation criteria meaning that they measure what is aimed to be measured. Finally, in order to fully understand the theoretical models of governance within the field of cybersecurity a systematic assessment of actor roles should take place in academia.

Bibliography

Badie, Bertrand. "Transnationalizing diplomacy and global governance." In *Diplomacy in a Globalizing World* (Second ed.), 90-109. New York: Oxford university press, 2018.

Carr, Madeline. 2015. "Power Plays in Global Internet Governance." *Millennium-Journal Of International Studies* 43(2): 640-59.

Casalini, Francesca, and Stefania Di Stefano. 2018. "State behaviour in cyberspace: moving away from a military discourse." *DiploFoundation.* Accessed 18 May, 2019. Available at: https://www.diplomacy.edu/blog/state-behaviour-cyberspace-moving-away-military-discourse.

Cohen, Raymond. "Diplomacy through the Ages." In *Diplomacy in a Globalizing World: Theories and Practices* (Second ed.), 21-36. New York: Oxford university press, 2018.

Cooper, Andrew F. "The changing nature of diplomacy." In *The Oxford handbook of modern diplomacy*, 35-53. Oxford University Press, 2013.

"Cybersecurity Tech Accord | Cybersecurity Tech Accord". 2018. *Cybertechaccord.Org*. Accessed 18 May 2019. Available at: https://cybertechaccord.org/accord/.

Deitelhoff, Nicole, and Klaus Dieter Wolf. 2013. "Business and human rights: How corporate norm violators become norm entrepreneurs." In *The Persistent Power of Human Rights: From Commitment to Compliance*, 222-238. Cambridge Studies in International Relations; 126. Cambridge: Cambridge University Press, 2013.

DeNardis, Laura. "The Internet Governance Oxymoron." In *The Global War for Internet Governance, 1-32*. New Haven: Yale University Press, 2017.

Droege, Cordula. 2012. "Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians." *International review of the Red Cross* 94(886): 533-578.

Eichensehr, Kristen. 2018. "Digital Switzerlands." *Available at SSRN* 1-66. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3205368.

Farer, Tom. "Diplomacy and International Law." In *The Oxford handbook of modern diplomacy*, 493-509. Oxford University Press, 2013.

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

France Diplomatie. 2019. "Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace." *France Diplomatie.* Accessed 22 April 2019. Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Froissart, Axel. 2019. "OECD Forum 2019 Session: From Territorial to Functional Sovereignty: Competition in he Digital Age." *The Forum Network.* Accessed 2 June 2019. Available at: https://www.oecd-forum.org/users/44536-axel-froissart/posts/49134-oecd-forum-2019-session-from-territorial-to-functional-sovereignty-competition-in-the-digital-age.

Gellman, Barton, and Laura Poitras. 2013. "U.S., British Intelligence mining data from nine U.S. Internet companies in broad secret program." *The Washington Post.* Accessed 2 June 2019. Available at: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.b39e963ab3f3.

Gerth, H. H., and C. Wright Mills. 1946. "Politics as a Vocation." *From Max Weber: Essays in Sociology* 77-128.

Gorwa, Robert, and Anton Peez. 2018. "Tech Companies as Cybersecurity Norm Entrepreneurs: A Critical Analysis of Microsoft's Cybersecurity Tech Accord." 1-25.

Grigsby, Alex. 2017. "The end of cyber norms." *Survival* 59(6): 109-122.

Grigsby, Alex. 2018. "The United Nations Doubles its Workload on Cyber Norms and not Everyone is Pleased." *Council on Foreign Relations.* Accessed 18 May 2019. Available at: https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

GCSC. 2018. "Global Commission Introduces Six Critical Norms Towards Cyber Stability – GCSC." *Cyberstability.Org*. Accessed at 31 March 2019. Available at: https://cyberstability.org/research/singapore_norm_package/.

Heine, Jorge. "From club to network diplomacy." In *The Oxford Handbook of Modern Diplomacy*, 54-69. Oxford University Press, 2013.

Hinck, Garrett. 2018. "Private-Sector Initiatives for Cyber Norms: A Summary." *Lawfare.* Accessed 28 May 2019. Available at: https://www.lawfareblog.com/private-sector-cyber-norm-initiatives-summary.

Hocking, Brian. "Rethinking the 'new'public diplomacy." In *The new public diplomacy*, 28-43. Palgrave Macmillan, London, 2005.

Hurel, Louise Marie, and Luisa Cruz Lobato. 2018a. "Unpacking cyber norms: private companies as norm entrepreneurs." *Journal of Cyber Policy* 3(1): 1-16.

Hurel, Louise Marie, and Luisa Cruz Lobato. 2018b. "Cyber-norms entrepreneurship? Understanding Microsoft's advocacy on cybersecurity." 1-16.

Charney, Scott, Erin English, Aaron Kleiner, Nemanja Malisevic, Angela McKay, Jan Neutze, and Paul Nicholas. 2016. "From Articulation to Implementation: Enabling Progress on Cybersecurity Norms." *Microsoft Corporation* 1-18.

International Committee of the Red Cross. 2019. "Mandate And Mission." *International Committee Of The Red Cross*. Accessed 18 May 2019. Available at: https://www.icrc.org/en/who-we-are/mandate.

Internet Governance Forum. 2019. "About the IGF." *Internet Governance Forum.* Accessed 28 May 2019. Available at: https://www.intgovforum.org/multilingual/tags/about.

Jacobsen, Jeppe Teglskov. 2017. "Denmark should avoid a 'Digital Geneva Convention'." *Royal Defence Danish College* 1-16.

Kerr, Pauline, and Geoffrey Wiseman. "Introduction." In *Diplomacy in a Globalizing World: Theories and Practices* (Second ed.), 1-18. New York: Oxford university press, 2018.

Kilovaty, Ido. 2019a. "Are Tech Companies Becoming the Primary Legislators in Cyberspcae?" *Lawfare.* Accessed 18 May 2019. Available at: https://www.lawfareblog.com/are-tech-companies-becoming-primary-legislators-international-cyberspace.

Kilovaty, Ido. 2019b. "Privatized Cybersecurity Law." *Available at SSRN 3338155* 1-51.

Lété, Bruno and Peter Chase. 2018. "Shaping Responsible State Behavior in Cyberspace." *The German Marshall Fund of the United States* 1-16.

Laudrain, Arthur P.B. 2018. "Avoiding A World War Web: The Paris Call for Trust and Security in Cyberspace." *Lawfare.* Accessed 31 March 2019. Available at: https://www.lawfareblog.com/avoiding-world-war-web-paris-call-trust-and-security-cyberspace.

Levy, David, and Rami Kaplan. "CSR and theories of global governance: strategic contestation in global issue arenas." In *The Oxford handbook of CSR*, 432-451. *The Oxford Handbook of Corporate Social Responsibility* (1st ed.). Oxford University Press. 2008.

Lijphart, A. (1971). "Comparative Politics and the Comparative Method." *The American Political Science Review* 65(3): 682-693.

Llorente, Vázquez Raquel. 2018. "A Digital Geneva Convention? The Role of the Private Sector in Cybersecurity." *LSE Ideas.* Accessed 31 March 2019. Available at: https://medium.com/@lseideas/a-digital-geneva-convention-the-role-of-the-private-sector-in-cybersecurity-cd96ecd70622.

Mačák, Kubo. 2017. "From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers." *Leiden Journal of International Law* 30(4): 877-899.

Mačák, Kubo. 2019. "On the Shelf, But Close at Hand: The Contribution of Non-State Initiatives to International Cyber Law." *AJIL Unbound* 113: 81-86.

Martinon, David. 2018. "In Brief: The Paris Call for Trust & Security in Cyberspace." *France Diplomatie.* Video File. Accessed 9 May 2019. Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

Matsakis, Louise. 2018. "The US Sits out an International Cybersecurity Agreement." *Wired.* Accessed 9 May 2019. Available at: https://www.wired.com/story/paris-call-cybersecurity-united-states-microsoft/.

Mayring, Philipp. 2000. "Qualitative Content Analysis." *Forum Qualitative Research* 1(2). Accessed 2 June 2019. Available at: http://www.qualitative-research.net/index.php/fqs/article/view/1089/2386.

Mayring, Philipp. "Qualitative Content Analysis." In *A companion to qualitative research* 3, 266-269. London [etc.]: SAGE, 2004.

McKay, Angela, Paul Nicholas, Jan Neutze, and Kevin Sullivan. 2014. "International Cybersecurity Norms: Reducing Conflict in an Internet-dependent World." *Microsoft Corporation* 1-22.

Melissen, Jan. "The new public diplomacy: Between theory and practice." In *The new public diplomacy*, 3-27. Palgrave Macmillan, London, 2005.

Microsoft. 2017. "A Digital Geneva Convention to protect cyberspace: Microsoft Policy Papers." *Microsoft Corporation.*

Microsoft. 2019. "Transparency Centers - Security Documentation". *Docs.Microsoft.Com*. Accessed 18 May 2018. Available at: https://docs.microsoft.com/en-us/security/gsp/contenttransparencycenters.

Mitnick, Drew. 2018. "Access Now to join the Paris Call for Trust and Security in Cyberspace." *Access Now.* Accessed 18 May 2019. Available at: https://www.accessnow.org/access-now-to-join-the-paris-call-for-trust-and-stability-in-cyberspace/.

Moulin, Thibault. 2019. "Paris Call for Trust and Security in Cyberspace: A Watershed Moment or a Storm in a Teacup?" *The Federmann Cybersecurity Center.* Accessed 18 May 2019. Available at: https://csrcl.huji.ac.il/people/paris-call-trust-and-security-cyberspace-watershed-moment-or-storm-teacup#_ftn4.

Neutze, Jan, and J. Paul Nicholas. 2013. "Cyber Insecurity: Competition, Conflict, and Innovation Demand Effective Cyber Security Norms." *Georgetown Journal of International Affairs*: 3-15.

Pasquale, Frank. 2018. "Digital Capitalism-how to Tame the Platform Juggernauts." *Friedrich-Ebert- Stiftung, Division of Economic and Social Policy* 1-4.

Pigman, Geoffrey Allen. "Debates about contemporary and future diplomacy." In *Diplomacy in a Globalizing World: Theories and Practices* (Second ed.), 72-89. New York: Oxford university press, 2018.

Pigman, Geoffrey Allen. "The diplomacy of global and transnational firms." In *The Oxford handbook of modern diplomacy*, 192-208. Oxford University Press, 2013.

Roy, Kritika. 2018. "Paris Call: Another Missed Call?" *Institute for Defense Studies and Analyses.* Accessed 9 May 2019. Available at: https://idsa.in/idsacomments/Paris-Call-Another-Missed-Call-kroy-181218.

Rudder, Catherine E., A. Lee Fritschler, and Yon J. Choi. "WHAT IS PRIVATE GOVERNANCE?" In *Public Policymaking by Private Organizations: Challenges to Democratic Governance*, 9-25. Washington, D.C.: Brookings Institution Press, 2016.

Sharp, Paul. "Diplomacy in international relations theory and other disciplinary perspectives." In *Diplomacy in a globalizing world. Theories and practices* (Second ed.), 57-71. New York: Oxford university press, 2018.

Smith, Brad. 2018. "An important step toward peace and security in the digital world." *Microsoft Blog.* Accessed 22 April 2019. Available at: https://blogs.microsoft.com/on-the-issues/2018/11/12/an-important-step-toward-peace-and-security-in-the-digital-world/.

Smith, Brad. 2017. "The need for a Digital Geneva Convention." *Microsoft Blog.* Accessed 18 May 2019. Available at: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/.

Soesanto, Stefan, and Fosca D'Incau. 2017. "The UNGGE is dead: Time to fall forward." *European Council on Foreign Relations.* Accessed 9 May 2019. Available at: https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance.

Streb, Christoph K. "Exploratory Case Study." In *Encyclopedia of Case Study Research*. 0 vol 1-4 Thousand Oaks, CA: SAGE Publications, Inc., 2010.

Thakur, Ramesh, Andrew F. Cooper, and Jorge Heiner. "Introduction: The challenges of 21st-century diplomacy." In *The Oxford handbook of modern diplomacy*, 1-31. Oxford University Press, 2013.

United Nations General Assembly. 2018. Resolution 73/266: Advancing responsible State behaviour in cyberspace in the context of international security (22 December 2018). *Resolution adopted by the General Assembly at its 65th plenary meeting.* Available at: https://undocs.org/pdf?symbol=en/A/RES/73/266.

United Nations General Assembly. 2018. Resolution 73/27: Developments in the field of information and telecommunications in the context of international security (11 December 2018). *Resolution adopted by the General Assembly at its 45th plenary meeting.* Available at: https://undocs.org/pdf?symbol=en/A/RES/73/27.

Walters, William. 2004. "Some critical notes on “governance”." *Studies in political economy* 73(1): 27-46.