Responsible Behaviour in Cyberspace: Engaging The Private Sector Through Tech Diplomacy

Author: Stefania Pia Grottola, Université de Genève (stefania.grottola@unige.ch)

Conference paper for the 17th Annual GigaNet Symposium

Draft article, do not cite

Abstract

In 2005, the Working Group on Internet Governance agreed that responsibilities arise among different stakeholders "in their respective roles" of shaping the evolution of the Internet (WGIG 2005, 4); however, their effective allocation, especially with regards to cybersecurity, relies on deeply politicized debates. The allocation of responsibilities, indeed, depends on how the notion of security in cyberspace is discussed as a priority by states and brought to security agendas. Building on the securitization theory by the Copenhagen School of International Relations, we argue that cybersecurity is conceptualized as a geopolitical means meant to shape policy-making processes and the responsibilities of relevant actors. Nevertheless, while the securitization process of cybersecurity helps in contextualizing the problem in the security sphere, it does not immediately provide a framework for responsibility allocation. This article aims at bridging this gap by advancing the following research question: «How are cybersecurity responsibilities created in the political discourse? And to what extent is the role of the private sector implemented in the quest for responsible behavior in cyberspace?» We propose an empirical foreign policy analysis of Canada, Netherlands, and Switzerland, and advance the following hypothesis: «The extent to which states engage diplomatically with the private sector varies with the establishment of cybersecurity as a foreign policy priority». We address the question through qualitative research methods of text analysis and semi-structured elite interviews and assess the correlation between the establishment of cybersecurity as an existential threat in the securitization paradigm and the turn to cybersecurity as a foreign policy priority. Finally, we look at the establishment of innovative forms of diplomatic engagement with the private sector and analyze its role as an intermediary in cybersecurity through the lens of the Orchestration-intermediary theory.

Keywords: cybersecurity, responsible behaviour, securitization, orchestration

Introduction

Societies worldwide are increasingly dependent on a series of strings made by 0s and 1s. Buzzwords such as *cyberspace* and *cybersecurity* are frequently employed to refer to a shared understanding yet deeply fractured and politicized. With the Internet becoming a backbone of international social, political, and economic relations, security studies are increasingly focusing on its vulnerabilities and how these are interlinked with traditional objects of security, expanding the cluster of emerging threats in security studies.

Providing security in cyberspace, generally referred to as *cybersecurity*, has posed important challenges to the traditional conceptualization of security from the identification of its referent objects to the provision of effective security management and the relevant actors involved. Indeed, while cybersecurity is a strategic national and international priority for Governments, they can hardly address the issue by themselves. A variety of (new) non-state actors is required for their expertise, resources, and principles. Nevertheless, the allocation of distributed responsibilities among stakeholders relies on deeply politicized debates.

A shared and internationally agreed-upon definition for *cyberspace* and *cybersecurity* has not been reached yet, leading to different framing by relevant actors fostering their agenda-setting objectives or foreign policy strategies. Defining cyberspace and delimiting the scope of cybersecurity creates a co-production of roles and responsibilities drawn not from binding mechanisms but from the legitimacy and accountability of the different stakeholders featuring the cybersecurity landscape. Allocating cybersecurity responsibilities indeed relies on politically connotated voluntary documents which explains why the question of responsibilities in cybersecurity is still lacking in global governance literature.

This article aims at bridging this gap by advancing the following research question: «How are cybersecurity responsibilities created in the political discourse? And to what extent is the role of the private sector implemented in the quest for responsible behavior in cyberspace?» We expect that the securitization of cybersecurity through the framing as an existential threat to national and international security increases cybersecurity relevance as a foreign policy priority. The provision of security in cyberspace represents an interesting case study of multi-stakeholder governance necessity as it is often recognized to be a shared effort among Governments and private tech companies producing and providing security systems. Therefore, we propose an empirical foreign policy analysis of Canada, the Netherlands, and Switzerland, and advance the following hypothesis: «The extent to which states engage

diplomatically with the private sector varies with the establishment of cybersecurity as a foreign policy priority».

Due to the politicized nature of the debate, the analysis looks at how state actors frame cybersecurity issues, what the related security measures entail, and how this creates relations, relationships, and therefore responsibilities for private sector actors. We complement this picture by looking at the extent cybersecurity is included as a foreign policy priority and the related degree of recognition of the role of the private sector in achieving such goals.

Conceptualizing responsibilities in cyberspace

The concept of responsibility has largely been analyzed as part of political and philosophical debates taking different shapes according to the contexts it is discussed. The contemporary use of its notion in political and ethical discourses leads to a variety of meanings and «senses» (Lucas 1993). To discuss responsibilities for the provision of security in cyberspace we are forced to look at different forms of accountability, not based on a legally binding instrument. Therefore, far from a philosophical discussion of the notion, this article defines responsibility as a form of legitimacy based on expertise- and resource-based source of authority (Avant, Finnemore and Sell 2010) of the stakeholders involved, and their accountability to act in accordance with their different roles and capacities.

By using this approach, a necessary reference to cybersecurity as a «shared responsibility» must be introduced. Cyberspace, and as a result cybersecurity, governance should be framed into the proliferation of intergovernmental and transnational governance creating a new global framework made by a multiplicity of state and non-state actors (Held 2013).

As an indispensable pillar of modern society (Jayawardane *et al.* 2015), cyberspace and its critical infrastructure relies on a series of physical infrastructure mainly owned by the private sector (Radu 2019). Economic, social, and political relations take place in cyberspace, and its regulation and governance should underline the role of communities and individuals for their expertise not driven by market interests.

The exponential evolution of the Internet led to the growth of social, legal, and economic-related issues where non-state actors are interested in voicing their perspectives (Radu 2019). Held questions whether this enlargement reflects a diffusion of political authority despite the sovereignty remains in the hand of states (Held 2013). While answering this question is beyond the scope of this research, it creates a framework for analyzing the

emerging role of the so-called «global governors» in the global Internet governance efforts (Avant, Finnemore and Sell 2010). Defined as the sum of «collective efforts» meant to address global issues impossible to tackle by states in their national capacities (Ibid.), the global governance of the Internet necessarily involves non-traditional actors through a new liquid form of authority with «a lower degree of consolidation and a significant dynamism in the configuration of authority structures, often spurred by the informality and multiplicity of governance institutions and tools» (Krisch 2017, 2).

This has also been reflected in the regulatory shift of the field from hard law, exclusively implemented by state authorities, to soft law mechanisms, which allow to include «new(er) actors» such the civil society and businesses (Radu 2019). As the author explains, the «logic of actions pertaining to different actors involved in [Internet governance] constrains the design of new rules» (Ibid., 194). Recommendations, guiding principles and voluntary codes of conduct define the proliferation of soft law mechanisms in the governance of cyberspace and cybersecurity showing a redefinition of roles in which the legitimacy of the actors is directly proportionate to their roles (Wgig 2005, 4).

Cybersecurity responsibilities rely on the legitimacy, source of authority and related accountability (Belli 2015) of the different stakeholders involved; however, these rely on deeply politicized debates. How can we allocate responsibilities in the absence of legally binding instruments? The answer relies on how these responsibilities are created. This article looks at how the notion of security in cyberspace is framed as an existential threat under the Securitization theory paradigm and discussed as a foreign security priority where the role of the private sector is accepted as indispensable.

Securitization theory

A prominent theoretical approach that explains how a security priority is formed and brought to the policy-making agenda has been conceptualized by the Copenhagen School of International Relations, also referred to as securitization theory. The theory proposes a framework for analysis of how security is formed as an agenda-setting process focusing on a broad range of threats rather than on mere military-related issues (Ficthner 2018). In other words, it conceptualizes security as a way of «establishing relations and relationships» (Ibid.) emerging from the responses of different actors to security-related threats.

According to the Copenhagen School scholars, security is a response to existential threats that justify the use of force and the mobilization of special power (Buzan*et al.* 1998). As

such, security leads towards a process that brings politics beyond its established rules and moves a topic in a spectrum from the political to the security realm as a «special kind of politics» or «above politics» (Ibid., 23). In this spectrum, an issue could be framed as a nonpoliticized topic, which does not represent part of the public and policy debates; as a politicized issue, which represents the dialectic of political realms; to finally the «above politics» and securitized section of the spectrum where it identifies an issue as an existential threat to referent object(s) (Ibid., 24-25). As a result, the notion of security should be understood as a self-referential practice: an issue is framed as security-related and not because a real threat is necessarily in place (Ibid., 24). Such a process is developed through a speech-act move by a securitizing actor, standing in the position of authority, and advancing the grammar of existential threat(s) following a logic of survival. Security can be seen objectively, when a threat is real, or subjectively when the threat is perceived (Wolfers 1962, 151) as the result of a specific narrative.

The securitization of cybersecurity reflects this practice by framing cybersecurity as a national and international security issue. The increase in securitization moves by states leads to a higher relevance in cybersecurity as a foreign policy priority. The aim of this research is therefore to contextualize state and non-state actors in the scholarship of security studies in order to assess their potential influence as securitizing actors and their respective securitizing moves (Balzacq 2010) in defining the security narrative in cyberspace. In doing so, we acknowledge the key role played by traditional state actors and look at the emergence of the influence of the private sector and its necessary role to achieve cybersecurity as a foreign policy priority. This well links and introduces the second theoretical framework of this research: The Orchestrator-Intermediary Theory.

Orchestrator-Intermediary Theory

According to the Orchestrator-Intermediary Theory (O-i t), an entity «enlists and supports intermediary actors to address target actors in pursuit of [its] governance goals» (Abbott *et al.* 2012, 2). The orchestrator brings into the governance arrangements intermediaries instead of governing targets directly. In other words, one actor (the orchestrator) works through a second actor (the intermediary) to govern a third actor (the target) (Abbott *et al.* 2012). Therefore, orchestration is an indirect and soft mode of governance that perfectly create a framework of analysis for the multi-stakeholder nature of cybersecurity by explaining the role of non-state actors (civil society, tech industry, and technical community) as indispensable

intermediaries for achieving states' targets in the age of digital interdependence. States as orchestrators rely on intermediaries, in our case mainly the private sector, for its expertise, recognized authority over the development and self-regulation of technologies, and the legitimacy to be the first respondent in cases of security breaches (Bures and Carrapico 2017).

For the purpose of this research, we identify as «orchestrators» state actors «supporting and integrating a multi-actor system of soft and indirect governance mechanisms meant to address shared goals that none of the actors could achieve on their own» (K. W. Abbott et al. 2012, 3). To link this postulate to the multi-stakeholder nature of Internet governance, and cybersecurity as well, we recall that «the multi-stakeholder model is necessary. You can't have governments do it all because the expertise isn't there; you can't have the private sector doing it all because their values are commercial and market-based [...] but they have the core competencies. [While] the civil society ought to be the combination of values and competencies unaligned with market interests. [...] Each plays an indispensable role» (Alec Ross interview 2019). Therefore, we define non-state actors as necessary «intermediaries» for their technical expertise, resources, and legitimacy that governments are lacking and for the increase of private authority and regulation that is inevitable due to the complexity and rapid change of the technological landscape (Avant *et al.* 2010; Hall and Biersteker 2002).

Research Design

The distribution of responsibilities and the related establishment of a threshold of accountability for state and non-state actors have not been extensively covered in policy-making agendas and in the academic literature on global governance due to the deep political disagreement on the specificities of the topic. With the aim to provide a small contribution to this gap, this research plans to address the allocation of responsibilities in the provision of security in cyberspace highlighting how these emerge as entailed by the construction of cybersecurity issues.

To do so, this article relied on data from national (cyber)security strategies, cybersecurity thematic studies, position papers, recommendation papers, and official press releases. These sources were selected from a pre-established database curated by UNIDIR (Cyber Policy Portail). We accepted all typology of documents as a standardized practice of strategy publication is not available across countries. Additionally, only the most recent documents were included in the analysis for each case study to represent the latest position of the

country. These documents were coded through text analysis methods to identify the grammar of existential threats, as well as to assess the degree of cybersecurity as a foreign policy priority. Complementary data was collected through semi-structured elite interviews with representatives from the private tech sector, civil society, technical community, and Government representatives in Geneva.

The definition of cybersecurity as an existential threat leads toward a set of actions and foreign policy priorities meant to address the issue. As cybersecurity challenges cannot be tackled by states alone, the role of the private sector becomes increasingly influential. Therefore, we argue that the framing of cybersecurity as an existential threat leads to the legitimization of the role of the private sector. This research's goal is to explain the political co-production of roles and responsibilities in the provision of security in cyberspace by looking at the definitions proposed for cybersecurity focusing on the grammar of existential threats proposed by the sample of states. We aim at showing how the responsibilities emerge from the position of authority and legitimacy of the various stakeholders, and as a result of the creation of a security issue. In doing so we answer the question: «How are cybersecurity responsibilities created in the political discourse? And to what extent is the role of the private sector implemented in the quest for responsible behavior in cyberspace?» We propose an empirical foreign policy analysis of Canada, Netherlands, and Switzerland, and advance the following hypothesis: «The extent to which states engage diplomatically with the private sector varies with the establishment of cybersecurity as a foreign policy priority». We address the question through qualitative research methods of text analysis and semi-structured elite interviews and assess the correlation between the establishment of cybersecurity as an existential threat in the securitization paradigm and the turn to cybersecurity as a foreign policy priority. Finally, we dive into the latter by looking at the establishment of innovative forms of diplomatic engagement with the private sector (i.e. appointment of tech ambassadors) and analyze its role as an intermediary in cybersecurity through the lens of the Orchestration-Intermediary theory (Abbott 2009; Abbott *et al.* 2012) with the goal to advance theoretical and empirical understanding of diplomacy and create a preliminary tech diplomacy overview for interested governments and institutions.

A definition of cybersecurity

The concept of security in cyberspace was introduced in post-Cold War agendas as a form of reaction to the disruption of technology developments changing the geopolitical landscape. From a technical standpoint, cybersecurity is linked to the protection of the physical infrastructure and the physical infrastructures involving the information security triad of confidentiality, integrity, and availability (Tech expert interview 2019). The confidentiality ensures that pieces of information in transit are not read by third parties; the integrity element establishes a liability feature of the data involved; and finally, the availability feature sets a robust architecture as well as the possibility to always access such information (Sumra *et al.* 2014). Nevertheless, technical definitions do not fully grasp the complexity of cybersecurity lacking the interaction between human agency and technology.

From a merely technical framing developed by computer scientists in the 1990s, the notion has started to be increasingly cited as referring to the threats posed to society (Hansen and Nissenbaum 2009). Shifting the focus to human interaction with digital technologies, we move from information security to cybersecurity (Solms and Niekerk 2013). Nonetheless, further and more detailed conceptualizations of cybersecurity rely on deeply politicized debates.

Cybersecurity: from politicization to securitization

The large acceptance of how cyberspace risks and vulnerabilities (Kurbalija and Murphy 2016) affect traditional critical information infrastructures (Dunn Cavelty 2016) features cybersecurity as a new sector of security objects (Burgess 2016) in national and international security agendas. Controversies over a common definition for cybersecurity also stem from the fact that it represents a process, a method, rather than a defined field leading to diverse policy-making agendas. According to Ficther, various conceptualizations of cybersecurity, such as those examined by Nissenbaum (2005) and Dunn Cavelty (2013), suggest various - and occasionally nearly opposing - policy consequences.

In the context of information and communication technologies (ICTs), Nissenbaum examines two definitions of security: one referred to as "computer security" and characterized by an individual-focused computer science and engineering approach; the other referred to as "cyber security," emerging as a form of concerns of governmental security agencies (Nissenbaum 2005). The first vision of security recalls the information security paradigm,

implying the establishment of specific technical measures and protocol; the second one, however, addresses human agency in the malicious use of new technologies (Ibid.), necessitating the involvement of law enforcement and surveillance entities. These two security visions provide different focuses on the subject and on the threats (Ficthner 2018).

The instrumentalization of cybersecurity definitions is also analyzed by Dunn Cavelty, who addresses the «cyber-threat representations» and the discursive construction of these threats (2013) leading to political tensions and disagreement that either strengthen the link between cyberspace, state power, control, and order; or look at «the role of the state [as] a gardener and facilitator» (Ibid., 119). These differences in conceptualizations also emerged during the interviews: «Depending on how you understand cybersecurity, you will get a different answer» (Canadian Diplomat interview 2019). Cybersecurity is indeed an umbrella term difficult to define: «on a case by case, you can say that something affects cybersecurity, but [defining it] is quite difficult» (Private sector expert (b) interview 2019). It identifies specific threats and referent objects (Hansen and Nissenbaum 2009) in international security, and «is discussed in many organizations and fora [because] it has many different applications» (Dutch Diplomat interview 2019).

Ranging from the protection of critical information infrastructure to cybercrime[1] and cyberconflict[2], cybersecurity is a highly contested concept leading to the «construction of security issues» in cyberspace (Ficthner 2018).

The different political stands of various stakeholders and securitizing actors delimit and define cybersecurity. From a Canadian diplomat's perspective, «cybersecurity is a means […] and a tool of empowerment», especially but not limited to people who normally do not have a voice (interview 2019). Moreover, as a Swiss Foreign Affairs Officer adds, cybersecurity is a means to ensure a stable environment, in which all actors can benefit alike, and in which cooperation is boosted. The Swiss Federal Department of Foreign Affairs (FDFA) refers to the concept as «strategic cyber stability» among and within states: a peaceful environment, not used for power projections and military activities (interview 2019).

Conceptualizing cybersecurity as a means positions the topic in Buzan, Waever, and de Wilde's spectrum (1998, 23). Cybersecurity as a means identifies traditional referent objects leading towards securitization, ranging from the protection of the public core of the Internet

[1] A single definition for cybercrime cannot be provided; nonetheless, it generally refers to a form of crime committed through digital means with the aim to use a device as an instrument and/or as a target (Aghatiste 2006).

[2] A singular definition cannot be provided; nonetheless, it generally refers to a conflict between state and non-state actors through digital means (Healey 2018).

to the protection of individual's privacy online and to the protection of the stability of the digital realm that boosts the economy, to cite a few.

Mapping cybersecurity

As Ficther argues, the notion of securitizing actors can comprehend who «takes over responsibilities and tasks to ensure cyber security» (2018, 7). Through content analysis means, complemented by elite interviews with diplomats, we have looked at the definitions of cybersecurity, the grammar of existential threat, and finally the referent objects identified by the narrative of Canada, the Netherlands, and Switzerland.

The table shows how the diversification of referent objects identifies a variety of ways to securitize a specific aspect of cybersecurity, identifying different establishments of relations and relationships in such conceptualizations. Responses and security measures to specific issues create «relations between the entities and the actors involved» (Ficthner 2018, 3).

TAB. 1. *Cybersecurity definitions and grammar of existential threats*

State	Cybersecurity definition	Grammar of existential threat	Referent objects
Canada	Protection of digital information and the infrastructure on which it resides (Public Safety Canada 2018, 7).	The risks in the cyber world have multiplied, accelerated, and grown increasingly malicious (Public Safety Canada 2018, II).	- Digital information - Infrastructure on which the digital information resides
Netherlands	Measures to prevent damage caused by disruption, failure or misuse of ICT and to recover should damage occur (Nationaal Cyber Security Centrum 2018, 9).	It is precisely because every aspect of society – social and economic – increasingly depends on digital processes that digital attacks can directly damage our economy and threaten national security (Nationaal Cyber Security Centrum 2018, 9).	- National security - Society
Switzerland	Strategic cyber stability: the geopolitical strategic stability among and between states. Peaceful environment which is peaceful, not used for power projection or military activities (Swiss Foreign Policy Officer interview 2019).	[Cyber] threats are developing very dynamically. The most important drivers are digitalization, which is making our society and economy increasingly vulnerable to disruptions and failures of ICT systems, as well as the intensified threat situation due to the observed professionalization of attackers and the expansion of power politics into cyberspace (Swiss Federal Council 2018, 3)	- Indiependence and security of the country - Stable cyber environment

Note: Direct quotes from national strategies and/or interviews.

The growing processes of internationalization and privatization are two major developments that have been dictated by the development of new technologies, as well as the rising dependence and interdependence on them (Dunn Cavelty, Krishna-Hensel and Mauer 2007). Internationalization of cybersecurity practices links to our focus on foreign policy rather than internal security. Cybersecurity challenges cannot be delimited by national boundaries due to the interconnection between countries, societies, social and economic relations. Furthermore, cybersecurity as a sub-field within the broad internet governance umbrella mirrors the global governance nature of the challenges and the governance strategies involved. Privatization complements the previous trend and it can be developed as an explanation of how public-private partnerships (PPPs) are implemented in cybersecurity. PPPs are not just employed in cybersecurity, according to Carr, but they have been extensively used since the 1990s in the privatization of crucial national infrastructures for the benefit of governments' economies (2016).

The need for PPPs in the context of cybersecurity can be attributed to the need for states to act in accordance with the perception that they are the primary actor responsible for providing national security in a situation where the private sector handles 96% of the provision of services and digital assets and the expertise.

Cybersecurity by which means? The need for orchestration

Addressing the responsibilities involved in the provision of security in cyberspace might be contested for its broad scope. However, it allows the analysis of how different securitizing mechanisms feature the cybersecurity landscape.

Different arrangements of relations, relationships, and duties are implied by various definitions of what cybersecurity is and involves. In the case of ICTs and information security, stronger ties between the public and commercial sectors are in fact necessary. While governments are the responsible bodies expected to set a framework for defining baseline security standards as well as channels of information-sharing regarding current and potential vulnerabilities, the private sector has a responsibility to produce the most secure goods.

TAB. 2 *Cybersecurity as a foreign policy priority*

State	Cybersecurity as a foreign policy priority	Cybersecurity by which means?
Canada	- Advice and contribute to policy development on cybersecurity and cybercrime (Global Affairs Canada 2021, 13). - Exercise leadership to promote the rule of law at the UN and within other international organizations, including a strategic stability framework for cyberspace (Global Affairs Canada 2021, 13). - Increase attention on international law issues arising from cyber, digital and Internet developments, including on cyber security and cybercrime and Internet jurisdiction matters (Canada 2022, 16). - Envision a future in which all Canadians play an active role in shaping and sustaining our nation's cyber resilience (Public Safety Canada 2018, 2).	- Working together across governments, academia, and the private sector is necessary to address the cyber skills gap. Taking action now will allow us [...] to support Canadian cyber security and that [...] contribute to Canada's future prosperity (Public Safety Canada 2018, 24). - Private sector leaders will have a central role to play, as a collaborative effort is needed to ensure that all Canadians are as equipped as possible to prevent and respond to cyber threats (Public Safety Canada 2018, 27).
Netherlands	- Contribute to international peace and security in the digital domain. [...] including safeguarding human rights (Nationaal Cyber Security Centrum 2018, 23). - Respond immediately and appropriately, alone or as part of a coalition, to digital attacks by state actors and has offensive capabilities that contribute to deterrence(Nationaal Cyber Security Centrum 2018, 23). - Contributes to the mitigation of cyber threats from criminals and state actors, by investing in the development of capabilities of the global cybersecurity chain (Nationaal Cyber Security Centrum 2018, 23).	- [T]he NCTV[3] takes the lead in promoting and ensuring the improvement of cybersecurity in a cohesive manner, in conjunction with all the parties involved (public authorities, business community, science, civil society). However, the government cannot do this on its own. All parties may and must be expected to accept their responsibilities and contribute to make and keep the Netherlands digitally secure as part of a concerted effort (Nationaal Cyber Security Centrum 2018, 43).
Switzerland	- Step up cybersecurity and specify standards under international law (FDFA 2020, 13).	The protection of Switzerland against cyber risks is the joint responsibility of society, the private sector and the

[3] Dutch National Coordinator for Security and Counterterrorism.

	- Expansion of capabilities for information gathering and attribution (Swiss Federal Council 2018, 23). - Further develop specialist knowledge and information gathering capabilities for the early identification of cyber attacks and their authorship (Swiss Federal Council 2018, 23). - Expansion of information exchange with the private sector (Swiss Federal Council 2018, 23).	state, with responsibilities and competencies clearly defined and put into practice by all those involved (Swiss Federal Council 2018, 8).

Note: Direct quotes from national strategies and/or interviews.

Governments continue to have the capacity to enact cybersecurity laws and make policies in this area. It is up to them to put in place the frameworks necessary to ensure that minimum security requirements are met. They must consult with other parties involved in the cybersecurity landscape since they lack the necessary skills to come up with the most thorough policy measures. The industry must play a critical role in the consultation processes by contributing the knowledge that the public sector lacks. Additionally, IT businesses have an obligation to their users, as stated by one of the private sector experts interviewed: Their audience is made up of a worldwide dimension of clients, and it is their duty to operate in a way that is consistent with their principles (interview 2019). Questions of «how secure?» and «who establishes the security threshold?» remain still specifically unanswered, but they let us argue that to reach an enforceable result, all stakeholders need to be consulted. As a Canadian diplomat explained, «We need to engage with all the stakeholders to arrive at the best policy, and of course, this policy is easier to enforce if all the [stakeholders] accept that it is how you we want to regulate it» (interview 2019).

The provision of security in cyberspace is generally acknowledged to be a shared responsibility of all the stakeholders involved in the cybersecurity landscape, but the politicization of the debate undercuts efforts to find binding mechanisms that would allow for the co-production of roles and responsibilities by the involved stakeholders based on their authority and legitimacy. The table shows the explicit recognition of the role of the private sector in guaranteeing the provision of security in cyberspace as a means for the achievement of cybersecurity as a foreign policy priority. The need for the private sector as a necessary actor elevates its role to the extent it is increasingly engaged diplomatically by traditional diplomatic actors, and states. We identify this as a necessary action through orchestration means.

The need for orchestration

Security issues in cyberspace are increasingly rising from the more complex and technical environment. New non-traditional security actors are involved due to the need for more and more expertise and resources. While the authority and role of traditional state entities will not be completely challenged, a process of complexification and technification is developing,

which requires a new paradigm for the analysis of how to secure this new virtual space through means that require shared responsibilities among traditional and traditional actors.

Security issues in cyberspace are increasingly rising from the more complex and technical environment. New non-traditional security actors are involved due to the need for more and more expertise and resources. While the authority and role of traditional state entities will not be completely challenged, a process of complexification and *technification* is developing, which requires a new paradigm for the analysis of how to secure this new virtual space through means that require shared responsibilities among traditional and traditional actors.

We indeed confirm our hypothesis on the basis of the previous table and use orchestration to justify and interpret the results. As we mentioned in previous sections, the Orchestrator-Intermediary Theory (O-I T), identifies a practice where an entity «enlists and supports intermediary actors to address target actors in pursuit of [its] governance goals» (Abbott *et al.* 2012, 2). In other words, the orchestrator brings into the governance arrangements intermediaries instead of governing targets directly. On the basis of this analysis, we argue that the appeal to the private sector in cybersecurity reflects the need to converge political interests with technical expertise and resources in the hands of the private sector.

As the interviews with governmental representatives pointed out, cybersecurity endeavors require an active role and involvement of the private sector. “Cybersecurity is an additional domain of cooperation for the public and the private entities” (Swiss Foreign Affairs Officer interview 2019). Indeed, “We governments, we don’t own the technology; most of the policy-makers do not understand the technology, so our first partner in this has to be the private sector” (Canadian Diplomat interview 2019). And finally, as a Dutch diplomat further added, “For us, it is very important to involve [the civil society and the private sector]. […] It is important that they contribute to the discussions so that We have the right discussions” (Interview 2019).

Orchestration emerges from the need for multi-stakeholder governance and it is justified by the fact that the goal of ensuring security in cyberspace cannot solely be achieved by states as traditional security actors. “One implication of privatization is that private companies make sure that their systems are secure: it is their own responsibility. It becomes a national security concern, and ultimately, a governmental task if private actors fall short of securing information and communication technologies. Ultimately, ICT vulnerabilities can potentially be exploited for malicious cyber purposes. This is why, in Switzerland, you have PPPs, which

is the way Switzerland cooperates with critical infrastructure operators in supporting them to be as secure as possible" (Swiss Foreign Affairs Officer interview 2019).

Orchestration is necessary to achieve cybersecurity-related foreign policy priorities and justifies the practice of states approaching tech companies diplomatically. Indeed, establishing diplomatic representations in key innovation hubs (i.e. Silicon Valley) with the goal of engaging with tech companies shows how the role of the tech private sector is being recognized and legitimized by traditional state actors. Nevertheless, further analysis is needed on how this takes place such as Cyber and Tech diplomacy.

Conclusions

This article has attempted to address the distribution of duties in the absence of binding mechanisms by examining how they are generated through political act(s) by legitimate individuals holding positions of authority. The analysis was founded on the securitization theory, which served as a theoretical foundation for comprehending how security measures establish ties and partnerships. The establishment of exceptional measures does not automatically provide a framework for the distribution of responsibilities; therefore, analyses must be gleaned through a study of the fragmented political landscape of cybersecurity, even among like-minded actors. This is true even though it is able to contextualize the topic in the security realm.

The debate over cybersecurity challenges this theory because of the complexity of the issue and the constellation of actors involved. It does this by putting non-state and non-military actors in a position to securitize a problem and influence whether or not the audience accepts the associated security measures and what they entail. To evaluate the exceptionality and effectiveness of security measures, a new inquiry should be added: whose responsibility? This can be a further element to the query "security through what means?", expanding the analysis of security to the role, influence, and capabilities of non-traditional security actors, especially of the private sector. Shared responsibilities and actions among governments and private actors are required to address the cybersecurity challenge leading toward processes of orchestration. The latter, indeed, emerges as a response to the necessary multi-stakeholder governance and it is justified by the fact that the goal of ensuring security in cyberspace cannot solely be achieved by states as traditional security actors.

We argue that orchestration is an inevitable phenomenon in the governance of cybersecurity and in the pursuit of cybersecurity foreign policy priorities. However, further

analysis is needed on the internet involving non-state actors such as the private sector, as well as on the modalities of how this takes place such as Cyber and Tech diplomacy.

Annex interview methods

The majority of the experts interviewed for this article preferred to be cited anonymously. Further details are available in the following table.

TAB. 3 *Interview Methods Table*

Interviewee	Affiliation	Format	Date	Place
Canadian Diplomat	Canada	Semi-structured elite interview	5 April 2019	Geneva, CH
Dutch Diplomat	Netherlands	Semi-structured elite interview	24 April 2019	Geneva, CH
Swiss Foreign Office Officer	Switzerland	Semi-structured elite interview	7 February 2019	Online
Alec Ross	Independent expert	Semi-structured elite interview	9 April 2019	Geneva, CH
Tech expert	Civil society	Semi-structured elite interview	11 April 2019	Geneva, CH
Private sector expert (a)	Private sector	Semi-structured elite interview	10 April 2019	Geneva, CH
Private sector expert (b)	Private Sector	Semi-structured elite interview	9 April 2019	Geneva, CH

Bibliography

ABBOTT, KENNETH W., PHILIPP GENSCHEL, DUNCAN SNIDAL, and BERNHARD ZANGL. (2012) *Orchestration: Global Governance Through Intermediaries*. doi: https://doi.org/10.2139/ssrn.2125452

ABBOTT, KENNETH, and DUNCAN SNIDAL (2010) *International Regulation Without International Government: Improving IO Performance Through Orchestration*, in "Review of International Organizations". 5 February: 315–44. doi: https://doi.org/10.1007/s11558-010-9092-3

AGHATISE, JOSEPH. 2006. *Cybercrime definition.* Available at: https://www.researchgate.net/publication/265350281_Cybercrime_definition. Accessed on 26 April 2019.

ALEC ROSS, Former Senior Advisor for Innovation at the United States Department of State, interview by Stefania Pia Grottola. 9 April 2019.

AVANT, DEBORAH D., MARTHA FINNEMORE, and SUSAN K. SELL (2010) *Who Governs the Globe?*, in "In Who Governs the Globe?", 1-32. Cambridge: Cambridge University Press.

BALDWIN, DAVID A. (1997) *The Concept of Security*, in "Review of International Studies" 23:5-26.

BALZACQ, THIERRY (2010) *Securitization theory: how security problems emerge and dissolve*. London: Routledge.

BELLI, LUCA (2015) *A heterostakeholder cooperation for sustainable internet policymaking*, in "Internet Policy Review" 4 (2): 1-21.

BURES,OLDRICH, and HELENA CARRAPICO (2017) *Private Security Beyond Private Military and Security Companies: Exploring Diversity Within Private–Public Collaborations and Its Consequences for Security Governance* in "In Security Privatization: How Non-Security-Related Private Businesses Shape Security Governance", 1–19. doi: https://doi.org/10.1007/978-3-319-63010-6_1.

BURGESS, J. PETER (2016) *Introduction*., in MYRIAM DUNN CAVELTY and THIERRY BALZACQ., "The Routledge Handbook of Security Studies", 1-4. London: Routledge.

BUZAN, BARRY, OLE WAEVER, and JAAP DE WILDE (1998) *Security : A New Framework for Analysis*. Boulder CO: Lynne Rienner.

CANADIAN DIPLOMAT, interview by Stefania Pia Grottola. 5 April 2019.

DUNN CAVELTY, MYRIAM, and MANUEL SUTER (2009) *Public-Private Partnerships are no silver bullet: An explained governance model for Critical Infrastructure Protection,* in "International Journal of Critical Infrastructure Protection" 2:179-187.

DUNN CAVELTY, MYRIAM, SAI FELICIA KRISHNA-HENSEL, and VICTOR MAUER (2007). *Introduction: information, power, and security—an outline*, in "Power and Security in the Information Age Investigating the Role of the State in Cyberspace", 8-9. Burlington, USA: Ashgate Publishing Company.

DUNN CAVELTY, MYRIAM (2013) *From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse*, in "International Studies Review" 15 (1). doi: https://ssrn.com/abstract=2200862.

DUTCH DIPLOMAT, interview by Stefania Pia Grottola. 24 April 2019.

FICTHNER, LAURA (2018) *What kind of cyber security? Theorising cyber security and mapping approaches*, in "Internet Policy Review" 7 (2).

GLOBAL AFFAIRS CANADA (2021) *Departmental Plan 2021-2022.* Available at: https://www.international.gc.ca/transparency-transparence/departmental-plan-ministeriel/2021-2022.aspx?lang=eng. Accessed on 28 Feruary 2021.

GLOBAL AFFAIRS CANADA (2022) *Departmental Plan 2022–23*. AVailable at: https://www.international.gc.ca/transparency-transparence/departmental-plan-ministeriel/2022-2023.aspx?lang=eng. Accessed on 16 February 16, 2022.

HALL, RODNEY BRUCE, and THOMAS J. BIERSTEKER (2002) *The Emergence of Private Authority in Global Governance*. Cambridge University Press.

HANSEN, LENE, and HELEN NISSENBAUM (2009) *Digital Disaster, Cyber Security, and the Copenhagen School*, in "International Studies Quarterly" 53 (4): 1155-1175.

HEALEY, JASON (2018) *The State of the Field of Cyber Conflict*, in "Council of Foreign Relations". Available at: https://www.cfr.org/blog/state-field-cyber-conflict. Accessed on 23 April 2019.

HELD; DAVID (2013). *The Diffusion of Authority*, in THOMAS G. WEISS andRORDEN WILKINSON. "International Organization and Global Governance". 60-72. London: Routledge

JAYAWARDANE, SASH, JORIS LARIK, and ERIN JACKSON (2015) *Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance*, in "The Hague Institute for Global Justice".

KRISCH, NICO (2017). *Liquid Authority in Global Governance*, in "International Theory" 9 (2): 237-260.

KURBALIJA, JOVAN, and MARY MURPHY. 2016. *An Introduction to Internet Governance.* 7th. Geneva: DiploFoundation; DiploCentar.

LUCAS, JOHN RANDOLPH (1993). *Responsibility*. Oxford: Oxford University Press.

NATIONAAL CYBER SECURITY CENTRUM (2018). *National Cybersecurity Agenda - Publication - National Cyber Security Centre*. Available at: https://english.ncsc.nl/publications/publications/2019/juni/01/national-cyber-security-agenda. Accessed on 20 April 2018.

NISSENBAUM, HELEN (2005). *Where computer security meets national security*, in "Ethics and Information Technology" 7: 61-73.

PRIVATE SECTOR EXPERT (a), interview by Stefania Pia Grottola. 10 April 2019.

PRIVATE SECTOR EXPERT (b), interview by Stefania Pia Grottola. 9 April 2019.

PUBLIC SAFETY CANADA (2018) *National Cyber Security Strategy: Canada's Vision for Security and Prosperity in the Digital Age*. Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx. Accessed on 21 December 2018.

RADU, ROXANA (2019). *Negotiating Internet Governance*. Oxford: Oxford University Press.

SOLMS, ROSSOUWVON, and JOHANVAN NIEKERK (2013). *From information security to cyber security*, in "Computers & Security" 38: 97-102.

SUMRA, IRSHAD AHMED, HALABI BIN HASBULLAH, and JAMALUL-LAIL AB MANAN (2014). *Attacks on Security Goals (Confidentiality, Integrity, Availability) in*

VANET: A Survey. Vehicular Ad-hoc Networks for Smart Cities: First International Workshop.

SWISS FEDERAL COUNCIL (2018). *National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018-2022*. Available at: https://www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html. Accessed on 2 February 2019.

SWISS FOREIGN AFFAIRS OFFICER, Swiss Federal Department of Foreign Affairs (FDFA), interview by Stefania Pia Grottola. 7 February 2019.

TECH EXPERT, interview by Stefania Pia Grottola. 11 April 2019.

WOLFERS, ARNOLD (1962). *Discord and Collaboration: Essays on International Politics*. Baltimore: Johns Hopkins University Press.