Proliferation of Cyber Norms: the Limitations of Traditional Diplomacy in Discussing Cyberconflict

Author: Stefania Pia Grottola, *Global Studies Institute* (Université de Genève)

September 2020

Conference paper for the 15th Annual GigaNet Symposium November 2, 2020.

Draft article, do not cite

Abstract

In 2017, the United Nations Group of Governmental Experts (UN GGE) failed to produce a consensus report witnessing the creation of the Open-Ended Working Group (OEWG) and the emergence of multi-stakeholder means of norm-entrepreneurship and political dialect. Moving from this abundance of proposed principles and norms, and using the Orchestrator-Intermediary theory as a theoretical framework, this analysis is led by the research question: *What does the abundance of cyber norms by multistakeholder intermediaries show about the limitations of existing institutionalized processes?* This paper uses qualitative research methods of textual analysis to subsume a purposive sample of cyber norms proposals and compare them for empirical analysis. In doing so, it contextualizes such abundance as a result of an inefficient inclusion of relevant stakeholders in institutionalized processes, framing these actors as potential orchestrators on the basis of a three-level stage of political engagement. Finally, it advances recommendations for better coordination mechanisms proceeding institutionalized consultations and addressing non-state actors overlapping efforts.

Introduction

As the militarization of cyberspace increases, discussions on responsible behaviour have been key points in the agenda of the United Nations Group of Governmental Experts (UN GGE). Important results were achieved by the consensus reports of 2013 (A/68/98*) stating that international law applies to cyberspace, and in 2015 (A/70/174) with the proposal of a set of voluntary norms, principles, and confidence-building measures. However, concerns emerged on the effectivity of voluntary norms and on the dangers that not agreeing on *how* international law applies can bring, especially on the resort to kinetic means after a cyber-attack. Indeed, the most recent work of the UN GGE failed to produce further results witnessing the creation of an additional group, the Open-Ended Working Group (OEWG). Despite the consistently different membership, the two groups' mandates largely overlap showing gridlocked shadows in cyber norms development.

Very little attention has been focused on critical indicators such as the disaggregated efforts to continue the work of norms recommendations in different fora. Diversified and at times disaggregated efforts have indeed been advanced by different – especially industry - stakeholders in the proposal of cyber norms through norm-entrepreneurship and the use of a political dialect. The Global Commission Stability of Cyberspace (GCSC), a multi-stakeholder initiative, has advanced the proposal for voluntary norms on responsible behaviour (GCSC 2018) based on the "protection of the public core of the Internet" which nowadays resonates in regional cybersecurity approaches. One of the GCSC's founders and major private sector actors in the field, Microsoft Corporation, has advanced the proposal of a Digital Geneva Convention under the cyber-law approach, in addition to other initiatives such as the Cybersecurity Tech Accord and the Digital Peace Now Campaign. Similarly, other private sector initiatives have been advanced by Siemens (Charter of Trust for a Secure Digital World), and Google (New Legal Framework for the Cloud Era). This resulted in an abundance of recommendations, norms, and principles from different stakeholders. The witnessing of such abundance, especially with regard to the private sector norm entrepreneurship in the proposal of principles with the aim of influencing policy-making make us wonder whether this can lead to a delegitimization of existing institutionalized processes where multi-stakeholder inclusion is limited – when present - to intersessional meetings.

Inexistent in the UN GGE and limited to a highly contested consultative process in the OWEG, this heterogeneous landscape of stakeholders and their advanced proposals raises the question of whether crucial actors are effectively involved in the consultations. Moving from this scenario, we puzzle our research interest on what an abundance of cyber norms can show about the potential limitations of existing institutionalized processes through the following research question: *What does the abundance of cyber norms by multi-stakeholder intermediaries show about the limitations of existing institutionalized processes?*

Challenging the traditional theorization of the Orchestrator-Intermediary theory, we navigate the question of whether there could be a shift in the paradigm: in other words, we wonder whether there could be a stronger and more influential role for those intermediaries and whether they might be perceived as orchestrators. Discussing responsible behaviour in cyberspace brings diplomacy to the challenges of a deeply interconnected world relying on infrastructure largely owned and provided by private actors and securitized by groups of multi-stakeholder experts (i.e. CERTS). While indeed the primary role of states as norms-developers remains, governing responsible behaviour underlines that this scope is not fully dominated by the rule of law and its enforcement, but also by a constant responsibility of all stakeholders in the respect, due diligence, naming and shaming of breaches and perpetrators.

The structure of this paper is articulated into three main sections. In the first section, we introduce the state of the art of scholarly literature on the importance of a multi-stakeholder approach to the governance of the Internet and to the discussions on security and responsible behaviour in cyberspace. We then contextualize the process of norm development and underline the major findings in the recent analysis of *cyber* norms institutionalized processes. Complementing the latter, we then frame the parallel efforts of non-traditional policy-maker actors in the proposals of norms, principles, and code of conduct as norm entrepreneurs. We finally conclude the section introducing our leading theoretical framework. We argue that the governance of responsible behaviour in cyberspace can be understood through the lens of orchestration. The theory postulates that an entity (orchestrator) will prefer governing a target (cyber norms) with indirect modes of governance through intermediaries (the tech industry) for their influential role played as the major provider and owners of the Internet infrastructure and its enabled technologies.

In the second section, building on our research question, we proceed with the definition and delimitation of the leading concepts for our analysis as a means to define the used methodology. Indeed, to better contextualize the abundance of recommendations, we have subsumed the previously mentioned cyber norms proposals and coded them though textual analysis to make them comparable for empirical studies. In doing so we have created a database that allows us to point out overlapping norms and principles and to see whether the composition of the groups behind the development of cyber norms reflects the allocation of responsibility in ensuring that the norms are respected.

In the third section, we construct our analysis framing the abundance of cyber norms as the result of an inefficient inclusion of relevant stakeholders in institutionalized processes whose role moves from mere norm entrepreneurship to a potential role as orchestrators. Finally, we conclude by advancing recommendations for better coordination mechanisms that would precede institutionalized consultations and address non-state actors overlapping efforts.

Section 1 - Literature review

A multiplicity of actors in the governance of cyberspace

Discussions on the governance of cyberspace and responsible behavior in cyberspace are characterized by a relatively new global framework made of a multiplicity stakeholders acting towards the shaping of the international political agenda with their different voices, interests, and perspectives (Held 2013). As a backbone and integral part of modern social life (Radu 2019; Kurbalija and Murphy 2016), the rapid worldwide evolution of the Internet and its enabled technologies implied an exponential growth of social, legal and economic-related issues resulting in the rapid expansion of non-state actors' interest in voice their perspectives in the governance of cyberspace (Radu 2019). Questions have been raised on whether such an enlargement of actors reflects a diffusion of political authority despite the fact that the sovereignty remains in the hand of traditional state actors (Held 2013). While a definitive answer cannot be addressed, the question introduces the emerging role of "global governors" in global governance (Avant, Finnemore and Sell 2010). The latter is defined by the sum of "collective efforts" meant to address global issues which would have otherwise been impossible to be tackled by states in their national capacities (*Ibid.*), and therefore lead to the involvement of legitimized non-traditional actors such as but not limited to the civil society and the industry.

The extensive scholarship on multi-stakeholder participation in Internet governance (Belli 2015; DeNardis and Raymond 2013; Carr 2015; van Eeten and Mueller 2012; Mueller 2012) has shown that those actors can indeed boast of authority, defined as a form of social relationships emerging from the recognition of legitimacy by other actors in a given political and institutional landscape. Four types of source of authority can be recognized: institutional (or institution-based), derived by an established and recognized institutional structure; delegated (or delegation-based), expressed by the devolution of authority by another legitimate entity; expert (or expertise-based), relying on and boasting of specialized know-how; and principled (or principle-based), whose authority is recognized for its purpose-driven by specific principles, morals or values (Avant, Finnemore and Sell 2010; Belli 2015). The emerging role of non-state actors thus introduces a new global governance practice characterized by 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). Indeed, the evolution of governance mechanisms has shown a shift from hard law, exclusively implemented by state authorities, to soft law mechanisms, which allow to include "new(er) actors" (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).

The topic of introducing new rules in governing security and responsible behvaiour in cyberspace exemplifies such constraints in its international policy-making processes. As a result, the preference and shift to soft law mechanisms are at the core of the international cybersecurity dialogue through the use of normative instruments meant to advance shared views and expectations (Tikk-Ringas 2016).

Norms development

The preference of norms over treaties for responsible state behvaiour in cyberspace was seen by Western countries as a means to pursue stability through "a series of easily digestible rules based on existing international law" (Grigsby 2017, 111). The international negotiation processes on security and responsible behaviour in cyberspace reflect the debate over legitimate actors in cyberspace and underline the need to contextualize the responsibilities involved. While states remain the only legitimate policy-makers, the recognition of the crucial role of the private sector as providers of technologies, services, and expertise legitimazes their authority, justifies the development with the OEWG to include multi-stakeholder consultations with experts and practitioners[1], and frames non-state actors led norms proposals into the debate. In this section, we analyze the normative nature of state-sponsored norms and we use it to introduce and contextualize the scholarship on non-state actors playing the role of norm entrepreneurs.

[1] The mandate of the OEWG includes informal intersessional consultative meeting of the OEWG with industry, non-governmental organizations, and academia (A/RES/73/27).

The normative nature of the instruments proposed through the UN-mandated groups should be understood through the lens of power. Building on Carr's distinction of economic power, military power, and power over opinions (1962), and Galtung's definition of ideological power as the power of ideas (1973), Manners introduces the normative power of soft law instruments as the ability to shape the concept of "normal" (Manners 2002) and - we add – of what is expected as responsible behavior. Scholarly literature on normative power has often addressed it as a means of serving national interests (Berenskoetter 2010; Kehoane and Nye 1977; Finnemore 1996; Finnemore and Sikkink 1998; Rosenacre 1998) providing a framework of interpretation where normative power legitimatizes or not state power (Tikk-Ringas 2016). Nevertheless, looking at the experience of the UN GGE, its developments with the creation of the OEWG, and the emergence of numerous indicate a limitation in the applicability and efficiency of the *cyber* normative power of traditional actors.

It is crucial to notice that international negotiations on cyber norms assume that the approved norms fall within the IR interpretation of the concept, defined by a prescriptive and evaluative force and by its wide acceptance within a community (Erksine 2016). However, the prescriptive and evaluative connotations of the consensus approved norms by the UN GGE in 2015 (A/70/174) show that a deeper focus and delimitation is required. Erksine and Carr (2016) define the attempts and outcomes to develop norms governing security and responsible behaviour in cyberspace as "quasi-norms". Those can have normative aspirations especially when actors with particular interests seek to improve behaviour, conducts, and practices that pursue such interests and values. In other words, the often labeled "cyber norms" can end up identifying preferred principles rather than actual norms when they do not take into consideration the broader context in which those norms should be placed (*Ibid.*). At this point, we want to focus the attention on such broad complex landscape of governing cyberspace and we focus on who can effectively play the role of advancing principles, code of conduct, and norms.

Norm entrepreneurship

With the failure of the 2016-2017 UN GGE, normative state-led initiatives of governing security in cyberspace came to a halt. This was followed by an *abundance* of efforts by non-state actors in advancing non-binding norms. Among the most notable, the principle of "non-interference with the public core of the Internet" (GCSC 2018a) and the following Singapore Package (GCSC 2018b), as well as purely private-led initiatives from Microsoft (the Digital

Geneva Convention (2018) and Cybersecurity Tech Accord (n.d.)). Acknowledging that states remain the only formal authority to create new international legal regimes, we build on the multi-stakeholder approach in Internet governance and look at the role of non-state actors in influencing policy and legal efforts. The previously cited developments led by non-state actors have indeed shown a new dimension in the proposal of norms through norms entrepreneurship (Hurel and Lobato 2018). The engagement of corporate actors in influencing policy-making has already been analyzed under the umbrella of corporate diplomacy and lobbying (Asquer 2012; Ordeix-Rigo and Duarte 2009; Keck and Kathryn 1998). However, in this paper, we focus on the action of private actors as presenting themselves as legitimate actors with authority to influence and pursue specific values, conducts, and behaviours through norms influence and development.

The emergence and development of norms can be described through a “life cycle” made of three stages: emergence, cascade, and internationalization (Finnemore and Sikkink 1998). In the first stage, an actor promotes a principle, behaviour or conduct; in the second stage, the norm is pursued to be socialized by other actors; finally, in the third stage, the norm is recognized as *opinio juris* and internationally institutionalized as a standard (*Ibid.*). In this paper, we do not assess the legitimacy of non-state actors as norms entrepreneurs considering that - in the case of *cyber* norms development- is still a field dominated by state authorities (Kuerbis and Badiei 2017). However, we focus on the first two stages and on the increase of proposals for security and responsible behaviour in cyberspace. Such increase fits into the framework proposed by Hurel and Lobato in which “the entanglement of the horizontal (stakeholder groups involved) and the vertical (hierarchy) dimensions in cyber norm production constitutes a regulatory framework that can neither be seen as a cohesive playing field nor reduced to a mere dialectic relationship between robust or tacit agreements” (2018, 65). What is clear, however, is that the failure of the 2016-2017 UN GGE has justified a redefinition of roles in discussing cyber norms showing that while states remain the only policy-drafting authority, different actors can advance principles, values, and behaviour expectations, advancing at least the first two stages of a norm life cycle.

Major examples refer to the Singapore Norms Package of the Global Commission on the Stability of Cyberspace, Microsoft’s Digital Geneva Convention, and Siemens’ Charter of Trust. Nevertheless, the list of norms proposal by non-governmental organizations, transnational corporations, and advocacy networks is much more extensive. While some of them were codified[2], others remain part of this unstructured abundance which leads to potential delegitimization of institutionalized processes. The Global Commission Stability of Cyberspace (GCSC) has advanced the proposal for voluntary norms on responsible behaviour (GCSC 2018) based on the "protection of the public core of the Internet" which nowadays resonates in regional cybersecurity approaches. One of the GCSC's founders and major private sector actors in the field, Microsoft, has advanced the proposal of a Digital Geneva Convention under the cyber-law approach in addition to other initiatives such as the Cybersecurity Tech Accord and the Digital Peace Now Campaign. Similar other private sector initiatives have been advanced by Siemens (Charter of Trust for a Secure Digital World), and Google (New Legal Framework for the Cloud Era). Inexistent in the UN GGE and limited to a highly contested consultative process in the OWEG, this heterogenous landscape of stakeholders and proposals raises the question of whether crucial actors are effectively involved in traditional institutionalized processes. Therefore, moving from this scenario, we puzzle our research interest on what an abundance of cyber norms can show about the potential limitations of existing institutionalized processes.

Section 2 - Theoretical framework

This paper has touched upon the increasing influent role of the private sector in the development of cyber norms through entrepreneurship. In order to analyse this phenomenon, we need a theoretical paradigm that explains why the tech industry is fundamental despite not carring out states' authority of norms development *per se*. We believe that the Orchestrator-Intermediary Theory (O-I theory) represents a fitting theoretical paradigm as it moves from the premises of indirect modes of governance. However, before introducing our theoretical framework in more detail, we will proceed with the clarification of leading concepts of "governance", and "indirect governance".

Firstly, governance can be defined as an institutionalized form of collective actions aiming at the approval of consensus or agreement either in voluntary or binding forms (Levi-Faur 2012). With this definition, we can deconstruct governance into four dimensions: structure, referring to formal and informal institutionalized setting; process, encapsulating the policy-making dynamics; mechanism of compliance and control; and finally, strategy as the process of influencing decisions and outcomes (*Ibid.*). The heterogeneity of issues and the diverse

[2] As a result of the efforts by the GCSC, the EU has recognized the "public core of the Internet" as essential for the normal operation of the Internet (EU Cybersecutity Act) (Council of the European Union 2019, para. 23).

nature of the processes in place for developing measures of responsible behaviour in cyberspace make the governance of cyber norms the setting where strategic governance is most needed. Secondly, we refer to “indirect” governance when such activities are carried out through intermediaries, namely non-state actors. The question that emerges is who is influencing whom and for what targets? We will see that in the traditional O-I paradigm the orchestration role is mainly carried out by state actors through intermediaries, often non-state actors. Focusing on the abundance of cyber norms, we wonder whether there could be a stronger and more influential role for those intermediaries and whether they might be perceived as orchestrators.

In the Orchestrator-Intermediary Theory, 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, instead of directly governing a target, orchestrators carry out their governance arrangements through intermediaries. One actor, orchestrator, works through a second actor, intermediary, to govern a third actor, the target(s) (Abbott, et al. 2012). This framework allows us to contextualize the abundance of cyber norms explaining the crucial role of non-state actors-led initiatives and cyber norms proposals as indispensable intermediaries for achieving states’ targets of governing responsible behaviour in cyberspace.

In order to complement our delimitation of concepts used in this paper, we define “orchestrators” those 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” (Abbott, et al. 2012, 3). We also define “targets” as those entities affected by the outcome of cyber norms development processes. Building on Abbott and Snidal’s conceptualization of the O-I theory (2009), we consider these targets as “managing state” when the targets are the states and – for instance – their responsible behaviour in cyberspace, or “bypassing states” when the outcomes ask for more responsible behaviour form private entities in charge of the provision – and at times security – of the systems and technologies at the core of modern society and activities. It is undeniable that the influential role of intermediaries in Internet governance is the rule rather than the exception due to the complexity of the issues at stakes and the lack of a centralized organization able to delegate its discussions through a principal-agent model. While research on the role of non-state actors in Internet governance processes exists (Flyverbom and Bislev 2008; Radu 2019; Nye 2014; Levinson and Marzouki 2014), it is still limited and inconsistently analysed.

A traditional interpretation of the O-I theory would argue that states, as orchestrators, rely on intermediaries in the form of non-state actors for their expertise that outstands the large majority of public competences, recognized authority over the development and self-regulation of latest technologies, and the legitimacy to be the first respondent in cases of security breaches (Bures and Carrapico 2017). In other words, the appeal to the private sector usually reflects the need to merge political interests with technical expertise and resources in the hands of the private sector. Nevertheless, at a first sight of the nature and abundance of norms proposed, we wonder whether the aim of governing the target of responsible behaviour in cyberspace moves from a stronger interest of non-state actors (and mainly some private tech companies) and whether we could argue that as those actors are trying to influence the outcomes of cyber norms development in institutionalized processes. In other words, with a provocative question, we wonder whether there has been a shift between orchestrators and intermediaries.

Research Question

After this conceptual overview of the status of the art of cyber norms development, its relative scholarship, and the most fitting theoretical framework, we build on the open puzzle abovementioned and we advance the following research question:

What does the abundance of cyber norms by multistakeholder intermediaries show about the limitations of existing institutionalized processes?

In order to address this question, it is necessary for us to define and delimit the concepts that we propose. First, we define the concept of “cyber norms” and we highlight the disagreement over its meaning and delimitation; second, we define and operationalize what we conceptualize as “abundance” of cyber norms; finally, we identify the institutionalized processes as the United Nations-mandated processes that are currently in place to discuss the developments in the intersection of information communication technologies and international security, as well as responsible behaviour in cyberspace, namely the United Nations Group of Governmental Experts (A/RES/58/32) and the Open-Ended Working Group (A/RES/73/27).

Section 2 – Conceptual delimitation

Cyber Norms and Abundance of them

Discussions about cyber norms are growing both in the literature and in the diplomatic practice; however, little focus is often dedicated to the conceptual definition and delimitation of norms and their “cyber” connotation (Finnemore 2017). Such confusion can often be identified in the different understandings of norms from practitioners and scholars: contrasting decades of sociology and IR scholarly literature, diplomats tend to interpret norms strengthening their voluntary and non-binding nature (Maurer 2020).

With this regard, it is important to notice that norms fall under the so-called policy instruments category made of norms, principles, and laws. While distinguished, their interconnection allows us to better define the concept. Norms differ from principles as the latter are statements of facts creating a goal or vision that a group wants to achieve rather than shared beliefs. “Pursuing agreement on principles, as opposed to norms, may be politically attractive precisely because it allows some fudging about behavioral obligations. Articulating specific obligations for specific actors (that is, articulating norms) invites scrutiny and claims of accountability in ways that principles do not.” (Finnemore 2017, n.p.). Additionally, norms differ from laws as they are broader and have no legally binding nature. As a result, considered crucial due to their purpose of guiding behaviour and providing motivations for specific actions, norms are defined as “collective expectation[s] for the proper behaviour of actors with a given identity” (Katzenstein 1996, 5).

Despite this definition, it is empirically hard to recognize a norm but through indirect observation (Björkdahl 2002) when the expected behaviour is reached or maintained. In this definition, the nature of the norms can be the one of regulating, constituting, or enabling actors in their environment (*Ibid.*). Regulatory norms prescribe behaviours through “rules of the road” (Raymond 1997, 214) meant to influence policy making processes. Such norms are means to determine individuals’ preferences or to “understand the causal relationship between their goals and alternative political strategies by which to reach those goals” (Goldstein and Keohane 1993, 12). Constitutive norms - on the other hand - create new actors, interests, or categories of actions (Björkdahl 2002). Finally, some norms enable actions necessary for the achievement of a given goal - that otherwise would have not been possible. In other words, while regulative norms prescribe behaviors, constitutive norms give a sense to specific actions, whereas enabling norms justify and permit certain actions (*Ibid.*).

Cyber norms

Internationally, the UN has pushed for the creation of cyber norms through the promotion of collective expectations of responsible behaviour through cyber norms negotiations of the UN GGE and OEWG (Hurel and Lobato 2018). Regionally, organizations like the OAS, ASEAN, OSCE, and NATO have proposed norms fostering capacity building and regional cooperation for cybersecurity. Additionally, non-governmental organizations, international initiatives, as well as corporations have advanced proposals with the aim of influencing states' behaviour and their acceptance to proposed norms. The multiplicity of actors reflect the complexity of the issues and the redefinition of roles played by different actors (Radu 2019).

It should be noticed that while the norms proposed as an outcome of institutionalized processes (i.e. UN GGE) can be defined as such because they have a prescriptive and evaluative form and are widely accepted, this is not necessarily the case for norms proposed by non-state actors or international multistakeholder initiatives[3]. To this regard, not properly qualifying as norms, the latter represent principles and codes of conduct which we identify as "quasi-norms" following Erkisine's and Carr's conceptualization (2016). For the purpose of this paper, we will use the term "norms" to identify proper ones and *quasi*-norms, but we acknowledge the conceptual distinction that should be kept in mind. Therefore, we refer to cyber norms as those regulatory and enabling norms that express a collective expectation over - the yet undefined - responsible behaviour in cyberspace.

Abundance of Cyber Norms

As the term "abundance" can be misleading and too subjective for its measurement and interpretation, we operationalize the concept of "abundance of cyber norms" through the use of two indicators: the multiplicity of similar norms, in other words, the existence of more than one norm for the same aim or outcome; and the nature of those cyber norms and related initiatives.

[3] The Singapore package produced by the Global Commission on the Stability of Cyberspace (2008) saw a large support by a variety of different actors; however, the same cannot be said for private sector-led initiatives which are still strongly contested and debated.

When thinking about cyber norms, diversified and disaggregated efforts come to mind: from the work of the UN GGE, the norms proposed by the Global Commission on the Stability of Cyberspace, to the voluntary norms proposed by private actors such as the Cybersecurity Tech Accord, and the Charter of Trust, to cite a few. On a closer look at the norms proposed – as it will be shown in the methodology and analysis – some of the aims or expected outcomes are recurrent in more than one set of norms with complementary or additional connotations. We define those overlapping as “multiplicity of norms”. We recognize that those overlapping norms touch upon a differently mandated group of experts and stakeholders, and we acknowledge that some of those norms were meant to complement existing efforts – at times gridlocked. Nevertheless, we take the stand that such an overlapping can potentially delegitimize the institutional processes already in place. While some might argue that the abundance of norms strengthens the agreement over general aims and outcomes, we believe that lesser processes should be in place in order to allow the continuum of discussions and in order to build developments in a more structured way. With this, we do not minimize the work of complementary groups of experts and professionals, whose variety of expertise and stakeholders is essential in the context of cyberspace and responsible behaviour in cyberspace, but rather argue that those processes should be included in a more structured policy development architecture that presents specific recommendations to policymakers in the existing processes. We present some recommendations in the concluding section.

Another connotation that we focus on trying to determine whether we can conclude that there is an abundance of cyber norms is the nature of the initiatives and norms proposed. Indeed, we argue that a reiterative, complementary, or supplementary nature of the norms leads to an increase of similar norms that – despite the actors and processes behind – can create confusion when referring to cyber norms. Reiterative norms highlight the importance of recalling approved norms in settings and fora that were not contemplated in the norms development processes. This raises the question of the role of non-state actors as indispensable in the governance and securitization of cyberspace, as well as well introduces our upcoming considerations on the link between norm entrepreneurship and orchestration. The complementary nature of the norms, instead, underlines the inability or inefficiency of existing processes in developing how consensus-based norms actually apply. Finally, a supplementary nature of the proposed norms stresses the need to cover aspects on which traditional diplomatic agreement and consensus by state actors is not yet achieved.

In this regard, we recall that United Nations-mandated processes do not necessarily include the active participation of non-state expert stakeholders and when this is the case, it is at times limited to a list of statements for fostering further discussions and awareness. While we do not have the means to evaluate the effectivity of this multi-stakeholder participation given the limited timeframe, we are in the position to wonder whether the case of abundance of norms might suggest limitations of these existing processes.

The proliferation of cyber norms and their abundance with regards to some aims and outcomes show efforts from non-state actors in influencing and indirectly governing targets. On this note, we plan to complement the scholarship on norm entrepreneurs and evaluate whether non-state stakeholders – for their expertise and/or influential role in the production and provision of the critical infrastructure of the Internet – can be analysed as orchestrators in the Orchestration-Intermediary paradigm that will be our leading theoretical framework.

	Indicators	**Description**
Abundance of Cyber Norms	Multiplicity of similar norms	Existence of more than one norm for the same aim or outcome
	Nature of the initiatives and outcomes	Reiterative, complementary and/or supplementary nature of the cyber norms initiatives and outcomes

Table 1 - Abundance of Cyber Norms

Methodology

As we do not advance a hypothesis that needs to be tested, but rather present an open-ended exploratory question, we adopt qualitative research methods to explore the phenomenon of the abundance of cyber norms. Our analytical objective is to assess whether we can argue that there is an abundance of cyber norms and to find initial explanations for what causes them.

To better contextualize the abundance of recommendations, we have subsumed a purposive sample of cyber norms proposals (see Table 2) and coded them though textual analysis to make them comparable for empirical studies. The selected norms include those produced by existing processes with a mandate from the United Nations (i.e. UN GGE) and those norms that gather momentum and a lot of attention as being proposed by a multi-stakeholder group of experts and actors (i.e. Global Commission on the Stability of

Cyberspace), or major private sector actors (i.e. Microsoft, Google, Siemens). We then proceed with the textual analysis and the coding of those norms. In doing so we have created a database that allows us to point out overlapping norms and principles and to address our explanatory research question on the efforts of non-state actors in influencing and indirectly governing the development of cyber norms and the governance of responsible behaviour in cyberspace.

Actor	Proposed set of norms	Year
UN GGE	2015 Consensus Report (A/70/174)	2015
GCSC	Advancing Cyberstability - Norms Package Singapore	2017
Google	New Legal Framework for the Cloud Era	2017
Signatories technology companies[4]	Cybersecurity Tech Accord	2018
Microsoft Corp.	Digital Peace Now Campaign	2018
Siemens	Charter of Trust	2018

Table 2 - Sample of Cyber Norms Proposals

The empirical analysis that we carry out compares the multi-stakeholder led cyber norms development initiatives and outcomes with the cyber norms approved by consensus by the 2015 UN GGE (A/70/174). We take the latter as a term of reference given that the composition of the group and the nature of the outcome reflect the most traditional understanding of norms development. By comparing the non-state actors led cyber norms initiatives' outcomes we seek to look whether there is abundance and try to contextualize such abundance in the context of multistakeholderism development of roles and responsibilities in Internet governance and responsible behaviour in cyberspace; on the changing nature of voluntary (cyber) norms; and on the possible interpretation of non-state actors as norms entrepreneurs through the lens of orchestration. These three aspects will be the leading points in the analysis of this exploratory study.

[4] The list of signatories is available at https://cybertechaccord.org/about/

Section 3 – Preliminary results

In the following tables, we summarize the results of the textual analysis and highlight the abundance of similar norms as well as the nature of those norms for the purposive sample we identified for this analysis.

Reference	Code	Advancing Cyberstability – Norms Package Singapore	Cybersecurity Tech Accord	Digital Peace Now Campaign	Charter of Trust	New Legal Framework for the Cloud Era	Multiplicity of norms

2015 UN GGE Report – A/70/174 (para 13. (a))	International cooperation for cyber stability and security against the malicious use of ICTs	-	Cooperation for enhancing cybersecurity;
			Strong defense;
			Collective response
				Stop governments engaging in warfare	Innovation and co-creation;
					Joint initiatives;
					Regulatory framework
						-	YES

2015 UN GGE Report – A/70/174 (para 13 (b))	Consideration of relevant information in case of ICT incidents	-	Protection against the malicious use of ICT	-	-	-	YES
2015 UN GGE Report – A/70/174 (para 13 (c))	Territorial due diligence against the malicious use of ICTs	Prohibition of cyber operations by non-state actors	-	-	-	-	YES
2015 UN GGE Report – A/70/174 (para 13 (d))	Exchange of relevant information to tackle the malicious use of ICTs	-	-	-	Transparency and response	Accessibility for legitimate law enforcement investigations	YES
2015 UN GGE Report – A/70/174 (para 13 (e))	Respect of human rights in securing the use of ICTs	-	-	Stop governments engaging in warfare	User-centricity	Commitment to basiline principles of privacy, due process, and human rights	YES
2015 UN GGE Report – A/70/174 (para 13 (f))	Protection of the Internet's critical infrastructure	Non-interference with the public core of the Internet	No offense	-	-	-	YES
2015 UN GGE Report – A/70/174 (para 13 (g))	Awareness creating activities	Basic hygiene	Provision of information and tools for cyber threats; Capacity building	-	Education	-	YES
2015 UN GGE Report – A/70/174 (para 13 (h))	Response to appropriate request in the case of malicious use of ICTs	-	-	-	-	-	NO
2015 UN GGE Report – A/70/174 (para 13 (i))	Protection of the integrity of the supply chain	Prohibition of tampering with products and services in development and production; Prohibition of commandeering ICT devices into botnets	Protection of customers and users with security, privacy, and integrity by design;	-	Responsibility throughout the supply chain; Security by default	-	YES
2015 UN GGE Report – A/70/174 (para 13 (j))	Sharing vulnerability knowledge	Creation of Vulnerability Equities Process (VEP); Reduction and mitigation of significant vulnerabilities	-	-	-	-	YES
2015 UN GGE Report – A/70/174 (para 13 (k))	Protection of CERTS and CIRT	-	-	-	-		NO

Table 3 - Abundance of Cyber Norms

Nature of the norms and initiatives					
	Advancing Cyberstability – Norms Package Singapore	**Cybersecurity Tech Accord**	**Digital Peace Now Campaign**	**Charter of Trust**	**New Legal Framework for the Cloud Era**
Reiterative		x	x		
Complementary	x	x		x	x
Supplementary	• Protection of the electoral infrastructure			• Ownership of cyber and IT security; • Certification for critical infrastructure and solutions	

Table 4 - Nature of the norms and initiatives compared to the 2015 UN GGE Report

Analysis

Three levels of political engagement

In our exploratory question, we aim to assess whether we can conclude that an abundance of cyber norms is in place. As shown by Table 3 and 4, the abundance is not only present but articulated in different shapes that can be linked to the diversified nature of the proposed norms. In this section, we contextualize such abundance as a result of an inefficient inclusion of relevant stakeholders in institutionalized processes and we frame these actors not as mere norm entrepreneurs but as potential orchestrators on the basis of a three-level stage of political engagement.

The reasons behind such an abundance of cyber norms can be multiple but - given the limited time and resource of this paper – we focus only on its multi-stakeholder settings. While extensive literature has addressed the necessity of a multi-stakeholder approach to the governance of cyberspace (Belli 2015; DeNardis and Raymond 2013; Carr 2015; van Eeten and Mueller 2012; Mueller 2012), discussions on cyber norms do not give the required attention to the link between authority and legitimacy of non-state actors and their influence in shaping negotiations of cyber norms. This can be justified by the fact that norms development in cyberspace is still dominated by states (Kuerbis and Badiei 2017); however, looking at the experience in other international politics fields (Hall and Biersteker 2002), we can start some reflections based on the sample of norms that we have identified for this analysis.

The reiterative nature of the proposal advanced by private actors such as in the case of the Cybersecurity Tech Accord and the Digital Peace Now Campaign indicate a form of support to existing efforts meant to strengthen cooperation on the matter, as well as trying to stop - or at least limit - governmental engagement in *cyber*-warfare. Interestingly, the private sector engages in the use of a political dialect that if not completely unprecedented, is quite uncommon in the traditional business practice. We identify such practice as the first level of political engagement of non-state actors in the influence of norms development. The degree of such influence depends on the shared recognition among legitimate actors that the player supporting and *reiterating* those norms does that moving from a position of being the *first respondent* with a responsibility to protect users regardless of their citizenship or their nature (McKay, et al. 2014). We argue that this first level of political engagement shifts the paradigm of non-state actors as mere intermediaries to players with orchestrators-similar roles.

The complementary nature of the norms proposed introduces the second level of political engagement of non-state actors. In our sample, this is shown by the Singapore Package proposed by a multi-stakeholder initiative, the Global Commission on the Stability of Cyberspace, as well as by private sector-led proposals by Microsoft (Tech Accord) and Siemens (Charter of Trust). The complementary nature of the norms proposed by those actors underlines some limitations of existing processes especially with regard to how existing norms apply. This second level of non-state actors' political engagement introduces the question and reflections on whether non-state actors and their proposals based on expertise- and resource-based authority are effectively taken into considerations in the processes, or whether some upgrades are needed in order to meet the requirements of a multi-stakeholder based governance.

Finally, the supplementary nature of the proposed norms strengthens the need to cover aspects and issues that due to their complexity and potential political controversy are not part of the shared agenda. This is indeed the case of the protection of the electoral infrastructure, proposed by the GCSC, and of the proposals advanced by Siemens with the ownership of cyber and IT security and the certification for critical infrastructure and solutions. This third level of political engagement of non-state actors demonstrates the need to rethink and recontextualize the role of stakeholders in the governance of security in cyberspace. We argue that the proactive political role and dialect used by those actors indicate their shift from intermediaries to potential orchestrators in influencing the target of governing responsible behaviour in cyberspace.

In this paper, we have used the leading question of what the abundance of cyber norms indicates about the potential limitations of existing institutionalized processes. Firstly, we can argue that the recurrent reiterative, complementary, and supplementary nature of non-state actors' sponsored norms create abundance when identifying and delimiting cyber norms. Indeed, the absence of a structured process that groups the proposals or defines a means to present and discuss them in specific fora shows the dispersive connotations of the different proposals. A preliminary cause that we identify for this phenomenon falls within the lack of effective inclusion of legitimate stakeholders in the development of norms. While the OEWG includes multi-stakeholder intersessional meetings, these are often limited to a list of statements and to the willingness of state actors to keep the recommendations and proposals in mind when discussing norms further. If these meetings show an important upgrade in traditional diplomatic practice, it is still unclear whether these are actually effective in including crucial stakeholders' views in the processes. More extensive research is indeed needed on the role of non-state actors in supporting the development of norms in the governance of security and responsible behaviour in cyberspace.

Secondly, building on the recognition of the private sector as norms entrepreneur (Hurel and Lobato 2018), and on the previously identified three-level stages of political engagement, we advance a reflection on the role of non-state actors and the private sector's players identified in this study's sample as orchestrators in the influence of norms development for security and responsible behaviour in cyberspace. First, their authority and legitimization are based on expertise and resources; second, their business interests can be contextualized into the broader and shared aim to have a stable, secure, and resilient cyberspace where their activities can continue, their users feel safe and trust the systems, and their products or services are not used as a means of warfare or as a target of it. While this study supports the view of non-state actors as orchestrators for targets shared by state actors as well, more empirical and theoretical analysis is needed for a broader generalization of the phenomenon.

Merging the gap: the role of tech ambassadors and cyber representatives

As we already mentioned in this paper, we recognize that some overlapping norms touch upon differently mandated groups of experts and stakeholders and that some of those norms were meant to complement existing efforts – at times gridlocked. However, we argue that this overlapping creates abundance able to potentially delegitimize the institutional processes already in place as they come from legitimate non-state actors (Nye 2000; Rosenau 2002) with key roles in the production, provision, and maintenance of many of the technologies we use in our daily lives. Fewer proposals and processes could facilitate legitimate actors in keeping track of proposals, changes, and developments. With this, we do not mean to minimize the work of complementary groups of experts and professionals as their expertise and perspective are crucially indispensable. Rather, we argue that those processes should be included in a more structured policy development architecture. The effectivity of intersessional multi-stakeholder sessions is still debated; additionally, the abundance of proposals by non-state actors – mostly private tech corporations – reiterates not only the role and legitimacy of these actors but also a need for better coordination mechanisms able to bridge the gap among traditional diplomatic institutional processes and innovative norm entrepreneurship means in security and responsible behaviour in cyberspace. While proposing international institutional changes is utopic and unrealistic, we point the attention to national institutional changes that have started bridging such gap through the appointment of dedicated diplomatic figures meant to face and develop a dialogue in the emerging practice of corporate diplomacy. Including digital affairs as part of its foreign policy priorities, Denmark established a dedicated office with a global mandate to discuss digital issues and with three geographic locations (Palo Alto, California; Copenhagen, Denmark; Beijing, China). France and Australia opted for a representation based in the home country as part of the Ministry for Foreign Affairs. Other forms of non-traditional diplomatic representations see countries leveraging their consular and governmental agencies' presence in the technological hubs such as the Bay Area: this is indeed the case of countries such as but not limited to Switzerland (swissnex), Austria (Open Austria), and Japan (NEDO) (Horejsova, Ittelson and Kurbalija 2018). Additionally, organizations such as the Office of the High Commissioner for Human Rights (OHCHR) and the International Committee of the Red Cross (ICRC) have nominated a dedicated representative based in innovation hubs; while the UN Secretary-General announced the appointment of a UN Tech Envoy during the closing ceremony of the 2019 Internet Governance Forum (IGF) in Berlin, Germany. The list goes on.

We see the role of tech ambassadors and dedicated representatives to the tech industry as multiple and diversified according to their countries' strategic priorities; nevertheless, their role can be crucial in bridging the gap between, on the one hand, the traditional institutionalized and state-led policy development in cybersecurity and, on the other hand, the fast-moving tech industry producing and providing cutting edge technologies as well as politically-based proposed norms for regulating this new fast-evolving landscape they create and largely shape. Institutions created in an "analogical" world might struggle in keeping up with the speed of digital innovation as these face the increasing challenges of those technologies to security and democracy while potentially not fully understanding and stimulating their use for good. Norms development in the field of security and responsible behaviour in cyberspace shows that. Therefore, we see the role of tech ambassadors and cyber dedicated representatives as a means to bridge this gap by developing an unprecedented dialogue with private tech actors in the landscape of Internet-based technologies. While more research on the topic is needed, this can be seen as a means of advancing soft law mechanisms to better contextualize and discuss the phase of the emergence of a norm by any legitimate entrepreneur, and to eventually pursue its cascade among different state and non-state recognized actors in the landscape of Internet and cybersecurity governance.

Conclusions

In this paper, we started navigating the multiple and disaggregated efforts by multi-stakeholder actors in continuing the work of cyber norms development especially after the failure of the 2017 UN GGE in producing a consensus report. We were led by the research question *What does the abundance of cyber norms by multi-stakeholder intermediaries show about the limitations of existing institutionalized processes?* which aimed to contextualize some potential limitations of the two institutionalized processes we focused on (UN GGE and OEWG). Acknowledging that the list of those norms is extensive and continuously increasing, we have identified a purposive sample of norms in the proposals by the Global Commission Stability of Cyberspace (Advancing Cyberstability - Norms Package Singapore), Google (New Legal Framework for the Cloud Era), Microsoft (Digital Peace Now Campaign), Cybersecurity Tech Accord, and Siemens (Charter of Trust). While we have shared the contextualization of those actors as norm entrepreneurs, we have decided to use the Orchestrator-Intermediary theory as our leading theoretical framework with which we aspired to assess whether the role of orchestrator is played by non-state actors in a multi-stakeholder environment.

Through qualitative research methods of textual analysis we have coded them for empirical analysis as a means to compare them with the institutionalized outcome of the 2015 UN GGE norms (A/70/174). Framing the abundance of cyber norms as a result of the multiplicity of similar norms for the same aim or outcome, as well as the reiterative, complementary and/or supplementary nature of the norms, we have firstly framed the abundance of cyber norms as the result of an inefficient inclusion of relevant stakeholders in institutionalized processes whose role moves from mere norm entrepreneurship to a potential role as orchestrators. This can be stressed due to their authority and legitimization, based on their expertise and resources, as well as on the basis of the goal of having a stable, secure, and resilient cyberspace for the continuation of their business activities. On this basis, we have shown that the shift to non-state actors as orchestrators can be exemplified by a three-level stage of political engagement reflecting the three nature of cyber norms proposals (first, reiterative; second, complementary; third, supplementary). While this study supports the view of non-state actors as orchestrators for targets shared by state actors as well, we acknowledge the limitations of proposing a generalization of the phenomenon as more empirical and theoretical research is needed on the topic.

Secondly, while recognizing that the work of complementary groups of experts and professionals is indispensable for their expertise and perspective, we argued that a more structured policy architecture could better facilitate the bridging of the gap between traditional institutional processes and innovative norm entrepreneurship means. To this extent, we see the role of tech ambassadors and cyber dedicated representatives as crucial in developing an unprecedented dialogue with non-traditional norm entrepreneurs and mediating the traditional state-led policy developments in cybersecurity and the fast-moving tech industry production of cutting edge technologies as well as politically-based proposed norms.

Bibliography

Abbott, Kenneth Wayne, Philipp Genschel, Duncan Snidal, and Bernhard Zangl. "Orchestration: Global Governance through Intermediaries." Available at SSRN: https://ssrn.com/abstract=2125452 or http://dx.doi.org/10.2139/ssrn.2125452, 2012.

Asquer, Alberto. (2012). "What is Corporate Diplomacy? And, Why Does it Matter?" *Journal of Multidisciplinary Research* 4 (2012): 53-64.

Avant, Deborah, Martha Finnemore, and Susan K. Sell. "Who Governs the Globe?" In *Who Governs the Globe?*, by Deborah Avant, Martha Finnemore and Susan K. Sell, 1-32. Cambridge: Cambridge University Press, 2010.

Belli, Luca. "A heterostakeholder cooperation for sustainable internet policymaking." *Internet Policy Review* 4, no. 2 (2015): 1-21.

Berenskoetter, Felix. "Thinking about Power." In *Power in World Politics*, by Felix Berenskoetter and M.J. WIlliams, 1-22. New York: Routledge, 2010.

Björkdahl, Annika. "Norms in International Relations: Some Conceptual and Methodological Reflections." *Cambridge Review of International Affairs* 15, no. 1 (2002): 9-23.

Broeders, Dennis, and Bibi van den Berg. *Governing Cyberspace Behavior, Power and Diplomacy.* London: Rowman & Littlefield International, 2020.

Bures, Oldrich, and Helena Carrapico. “Private security beyond private military and security companies: exploring diversity within private-public collaborations and its consequences for security governance.” *Crime, Law and Social Change* (Springer International) 67, no. 3 (2017): 229-243.

Carr, Edward Hallett. *The Twenty Years' Crisis 1919-1939.* london: Macmillan, 1962.

Carr, Madaline. “Power Plays in Global Internet Governance.” *Millennium: Journal of International Studies* 43, no. 2 (2015): 640-659.

Council of the European Union. 09 04 2019. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2019-0151+0+DOC+PDF+V0//EN (accessed 04 11, 2019).

DeNardis, Laura, and Mark Raymond. "Thinking Clearly about Multistakeholder Internet Governance." *GigaNet: Global Internet Governance Academic Network, Annual Symposium 2013.* Bali, 2013.

Erksine, Toni. "Normative International Relations Theor." In *International Relations Theories: Discipline and Diversity*, by Tim Dunne, Milja Kurki and Steve Smith, 236-258. Oxford: Oxford University Press, 2016.

Erskine, Toni, and Madeline Carr. "Beyond ‘Quasi-Norms’: The Challenges and Potential of Engaging with Norms in Cyberspace." In *International Cyber Norms: Legal, Policy & Industry Perspectives*, by Anna-Maria Osula and Henry Rõigas, 87-109. Tallinn: NATO CCD COE Publication, 2016.

Finnemore, Martha. "Cybersecurity and the Concept of Norms." *Carniege Endowment for International Peace*, 2017.

—. *National Interests in International Society.* Ithaca, NY: Cornell University Press, 1996.

Finnemore, Martha, and Kathryn Sikkink. "Activists Beyond Borders: Advocacy Networks in International Politics." *International Organization* 52, no. 4 (1998): 887-917.

Finnemore, Martha, and Kathryn Sikkink. "International Norm Dynamics and Political Change." *International Organization* 52, no. 4 (1998): 887-917.

Flyverbom, Mikkel, and S. Bislev. "Internet regulation-multi-stakeholder participation and authority." In *Critical perspectives on private authority in global politics*, by Dorte Salskov-Iversen and Hans Krause Hansen, 72-90. Palgrave Macmillan UK, 2008.

GCSC, Global Commission on the Stability of Cyberspace. *Definition of the Public Core, to which the norm applies.* Bratislava: GCSC, 2018a.

GCSC, Global Commission on the Stability of Cyberspace. "Norm Package Singapore." 2018b.

Goldstein, Judith, and Robert O. Keohane. *Ideas and Foreign Policy: An Analytical Framework.* Ithaca, London: Cornell University Press, 1993.

Grigsby, Alex. "The End of Cyber Norms." *Survival* 59, no. 6 (2017): 109-122.

Gultang, Johsn. *The European Community: A Superpower in the Making.* London: Allen & Unwin, 1973.

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

Held, David. "The Diffusion of Authority." In *International Organization and Global Governance*, by Thomas G. Weiss and Rorden Wilkinson, 60-72. London: Routledge, 2013.

Horejsova, Tereza, Pavlina Ittelson, and Jovan Kurbalija. *The rise of techplomacy in the Bay Area.* Geneva: DiploFoundation and the Geneva Internet Platform, 2018.

Hurel, Louise Marie, and Luisa Cruz Lobato. "Unpacking cyber norms: private companies as norm entrepreneurs." *Journal of Cyber Policy* 3, no. 1 (2018): 61-76.

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

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

Kehoane, Robert O., and Joseph S. Nye. *Power and Interdependence.* Boston: Little, Brown, 1977.

Krisch, Nico. "Liquid Authority in Global Governance." *International Theory* 9, no. 2 (2017): 237-260.

Kuerbis, Brenden, and Farzaneh Badiei. "Mapping the cybersecurity institutional landscape." *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 466-492.

Kurbalija, Jovan, and Mary Murphy. *An Introduction to Internet Governance.* Geneva: DiploFoundation; DiploCentar, 2016.

Levi-Faur, David. *Oxford Handbook of.* Oxford: Oxford University Press, 2012.

Levinson, Nanette S., and Meryem Marzouki. "Internet Governance Institutionalization: Tensions and Trajectories." *23rd IPSA World Congress of Political Science*, 2014: 1-25.

Manners, Ian. "Normative Power Europe: A contradiction in terms?" *Journal of Common Market Studies* 20, no. 2 (2002): 235-258.

Maurer, Tim. "A Dose of realism: The Contestation and Politics of Cyber Norms." *Hague Journal on the Rule of Law*, 2020: 283-305.

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

Microsoft. "A Digital Geneva Convention." *Microsoft Policy Paper.* 2018. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH (accessed 03 26, 2019).

Mueller, Milton. *Networks and States: The Global Politics of Internet Governance.* Cambridge MA: MIT Press, 2012.

Nye, Joseph S. *Governance in a globalizing world.* Cambridge, Mass: Visions of Governance for the 21st Century, 2000.

Nye, Joseph S. “The Regime Complex for Managing Global Cyber Activities.” *Global Commission on Internet Governance* 1 (2014).

Ordeix-Rigo, Enric, and João Duarte. "From Public Diplomacy to Corporate Diplomacy: Increasing Corporation’s Legitimacy and Influence." *American Behavioral Scientist* 53, no. 4 (2009): 549-564.

Radu, Roxana. *Negotiating Internet Governance.* Oxford: Oxford University Press, 2019.

Raymond, Gregory A. "Problems and Prospects in the Study of International Norms." *Mershon International Studies Review* 41, no. 2 (1997): 205-245.

Rosenacre, Richard. "The European Union: A New Type of International Actor." In *Paradoxes of European Foreign Policy*, by Jan Zielonka, 15-24. The Hague: Kluwer Law International, 1998.

Rosenau, James N. *Information Technologies and Global Politics : The Changing Scope of Power and Governance.* Albany: State Univ. of New York Press, 2002.

Tech Accord. *Cybersecurity Tech Accord.* n.d. https://cybertechaccord.org/.

Tikk-Ringas, Eneken. "International Cyber Norms Dialogue as an Excercise of Normative Power." *Georgetown Journal of International Affairs* 17, no. 3 (2016): 47-59.

UN General Assembly. "Developments in the field of information and telecommunications in the context of international security." *A/RES/73/27.* 12 11, 2018.

UN General Assembly. "Developments in the field of information and telecommunications in the context of international security." *A/RES/58/32*. 12 18, 2003.

van Eeten, Michel JG, and Milton Mueller. “Where is the governance?” *New media & Society* 15, no. 5 (2012): 720-736.