Systems under Pressure:
Polities, Networks and International Cooperation for Cybersecurity

IPSA International Conference 2017
Political Science in the Digital Age

Louise Marie Hurel[i]
l.h.dias@lse.ac.uk

Carlos Frederico P D S Gama[ii]
carlosfredericopdsg@uft.edu.br

Introduction

In an Age of Information, cyber security systems grew exponentially in terms of scale and complexity. Scale. Complexity. As the Cold War drew to a close, cybersecurity claimed priority among the new security challenges. In computational terms, as complexity unfolds, dealing with each and every cyber security violation becomes less feasible and yet, the costs of casting a blind eye skyrocket. From financial markets to arms control systems, social vulnerability to cyber threats is also on the rise.

At the same time, international attempts to promote cybersecurity remained modest, amidst a host of polarizing political issues. As the Internet and information and communication technologies come closer to the center stage of political, economic, cultural and social dynamics, challenges and disputes regarding cybersecurity become an ever-more pressing issue. In this regard, the hacks on the Democratic National Committee during the 2016 US presidential campaign, concerns over external interference in French and German elections, vulnerabilities in widespread interconnected systems/devices share the spotlight of cybersecurity threats.

It is within this context that national governments are stuck in precarious positions. In socio-technical overlaps, other social agents have comparative advantages, which affect the structuring of military-cybernetic complexes and undercut the shadow of the future. The complexity of information systems and regulative limits of national governments provide incentives for international cooperation – the multiplication of violations and rising uncertainty increase mutual vulnerabilities between states and societies. Paradoxically, the level of international compliance in cybersecurity is remarkably low next to other security spheres (such as preventing the use of weapons of mass destruction).

This paradoxical situation builds on domestic fragilities (limited regulatory capacities by national governments) and produces three international outcomes of relevance to matters of global governance. Firstly, there is a situation of mutual vulnerability between states in cybersecurity. This could, as other security hazards, induce institutional buildup at the international level. Secondly, the expertise of private agents remains a decisive factor in decisionmaking: a challenge and an asset. Finally, international regulation remains precarious and compliance is low.

We propose that, in complex entanglements between private and public agents, preventing systemic meltdowns gain the upper hand next to curbing violations. In this context (low compliance, high risk), instead of coping with violations in national cybersecurity systems as they go (computationally unfeasible, at the risk of systemic meltdown), governments have incentives to provide reward to expert violators that act in advance. As governments lose ground to private agents in regulative terms and international bodies remain non-decisive on the matter, social dynamics depart from international standards of protection to private-public preventive action.

Our focus, therefore, will be the set of challenges to international cooperation for cybersecurity. In order to do so, we shall also analyze the developments of the United Nations Group of Governmental Experts (UNGGE), G7 and other international initiatives related to cybersecurity. This paper builds on an extensive mapping of international and bilateral agreements on cybersecurity. Thus, the purpose of this paper is to question whether international norms for cybersecurity is a feasible and perhaps desirable road for states to pursue.

Turbulence in World Politics and Cybersecurity

"*Governments need to recognize the amazing benefits of the Internet, and do nothing to cripple it*"(United States Internet Council, 2000)[1]

"*I'm willing to sacrifice all of that because I can't in good conscience allow the US government to destroy privacy, internet freedom and basic liberties for people around the world with this massive surveillance machine they're secretly building*" (Snowden, 2013)[2]

By the early 2000s, the US government was taking the lead in keeping Internet both loosely regulated (through a private American entity, ICANN) and tightly under its control (blocking international regulation through the UN system or even a pool of national agencies, affording other countries few options, like restricting Internet provision or nationalizing transcontinental optical cables). The Clinton administration fought to keep this status quo in international for a (including the infant World Trade Organization). 2000 was considered the year the "Internet bubble" reached its apex (with NASDAQ reaching an all-time high). Notwithstanding Internet's genealogy as a military network during the gloomy days of Cold War (the ARPANET – devised as a strategic computer network that would survive a Soviet nuclear attack), Internet was an economic asset, rather than a national security matter (KOBRIN, 2001). Policy and academic debates revolving over self-regulation of e-markets rather than over the policy implications of an overcrowding network extending across continents during an era of *turbulence in world politics* (Rosenau, 1990). Internet and international relations met in events such as Peter Arnett's live transmissions for CNN from Iraq and Somalia in early cellphones and limited range connections; so-called "CNN Effect" (Robinson, 1999) that could have affected US decision to intervene in Somalia was due to the earliest inceptions of a "worldwide" web by then largely limited to the US and close allies.

[1] http://edition.cnn.com/2000/TECH/computing/09/01/state.of.the.net.01/index.html

[2] http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance

Elsewhere, also in 2000 the Brazilian government created the first policy orientations for dealing with Internet in terms of security. Considering "*cybersecurity and cyber defense strategic vectors for the state*"[3] a Data Security Police was framed by Brazilian National Defense Council. By then, China had slowly receding from the events of Tiananmen Square; its Internet connections were duly operatives by nowadays' patterns, but Chinese users were receiving massive state incentives to join the global bandwagon (not to mention register with government-run Internet providers). The same took place, in a more modest scale, in South Africa, in which the digital divide was only one of the many divides legated by the Apartheid. For long considered computer science households, Russia (even after the USSR's demise) and India would wait some time before being counted among the most vibrant societies in terms of Internet usage – even though a much larger share of population was digitally included in the former than in the latter. Russia by then has barely 10 million Internet users and the government was disinterested in regulating this tiny networld (even though since 1994 attempts have been made to do so), what made Russia a de facto piracy paradise for some time. On the contrary, by 2000 India incepted its Information Technology Act – a restrictive legislation allegedly triggered by Pakistani bloggers and hackers (it was only three years after nuclear explosions on both sides of Jammu-Kashmir contested borders).

Some years in advance, according to the International Telecommunication Union (ITU), the Internet amassed 2.7 billion users; there were also 7 billion cellphones all over the world (ITU, 2013). That year Brazilian President Dilma Rousseff had her cellphone wiretapped and her electronic mailing violated, alongside other heads of state and government, by US' National Security Agency (NSA) during UN and G8 meetings. Information and Communication Technologies (ICT) had already become stalwarts of contemporary warfare. During the Obama administration, major contingents of US troops withdrew from Afghanistan and Iraq, but warring efforts remained. In those places (and also in Yemen and Somalia) drones were in charge of targeting terrorists, sometimes qualified as a "global apparatus" involving "*…dozens of secret facilities, including two operational hubs on the East Coast, virtual Air Force cockpits in the Southwest and clandestine bases in at least six countries on two continents*" [4]. Now comprising the BRICS group, Brazil, Russia, India, China and South Africa actively refused to take part in US-led intervention efforts in Libya and Syria (by casting negative or absent votes in the United Nations' Security Council, by blocking political negotiations that would facilitate interventions, humanitarian or not, and by actively calling for reforms in political and economic international institutions).

In-between, the Internet experienced three dramatic shifts. Firstly, the "Internet bubble" burst in early 2002. As the ensuing financial crises followed, Internet and correlate technologies become a matter of international economic polemics, a global challenge. Partly coordinated through Internet, the terrorist attacks of September 11 2001 were a turning point in bringing governmental attention to what citizens did in the web apart (and in its interstices, the deep web). Across the 2000s, Internet allowed coordination of contestation in the Arab Spring and played a decisive factor in catalyzing Barack Obama's donations and public profile.

[3] http://www.sae.gov.br/site/wp-content/uploads/relatorio_XIIIENEE_ebook.pdf, p.17

[4] http://www.washingtonpost.com/national/national-security/under-obama-an-emerging-global-apparatus-for-drone-killing/2011/12/13/gIQANPdILP_story.html

Associating digital inclusion with human rights and the empowerment of civil society, the Brazilian government considered the NSA scandal revealed by Edward Snowden an infringement of basic rights and a breach of Brazilian sovereignty. President Rousseff took the initiative to bring the issue to the headlights during the UN's General Assembly opening ceremony – after cancelling a long-planned high-level Presidential trip to US, the first of a Brazilian head of state since 1995. Before the UN President Rousseff launched the seed of a multilateral initiative to curb cyber espionage through Internet regulation[5]. The initiative ignited when German Prime Minister Angela Merkel (who had also been targeted by NSA) co-sponsored with Rousseff a General Assembly resolution on the right to online privacy and cybersecurity in November. In 2014, a high-level conference in São Paulo, Brazil announced a multi-stakeholder framework for Internet regulation. NETmundial's final *Multistakeholder Statement* explicitly outlined the security, stability and resilience of the Internet as one of the guiding principles to global Internet governance:

> *Security, stability and resilience of the Internet should be a key objective of all stakeholders in Internet governance. As a universal global resource, the Internet should be a secure, stable, resilient, reliable and trustworthy network. Effectiveness in addressing risks and threats to security and stability of the Internet depends on strong cooperation among different stakeholders.* (NETMUNDIAL, 2014)

An emerging concept in international relations, cybersecurity partakes in the widening and deepening of security issues after the Cold War, a move that was associated by many IR scholars with the unprecedented peaceful end of the bipolar rivalry, the emergence of non-state threats in a turbulent world, reflections upon the state as a constructed entity and new technologies used in conflict and warfare. Hansen and Nissenbaum (2009, p. 1155) depict the "arrival" of cybersecurity in IR studies in those terms:

> "*Cyber security was first used by computer scientists in the early 1990s to underline a series of insecurities related to networked computers, but it moved beyond a mere technical conception of computer security when proponents urged that threats arising from digital technologies could have devastating societal effects. Throughout the 1990s these warnings were increasingly validated by prominent American politicians, private corporations and the media who spoke about ''electronic Pearl Harbors'' and ''weapons of mass disruption'' thereby conjuring grave threats to the Western world*"

Cybersecurity involves security activities in a digital environment considered strategic to a social agent – be a state, a corporation, a non-governmental organization, a bunch of citizens etc. (Dunn Cavelty 2013, 109). It fuses a technical (supposedly innovative) discourse on ICT with (usually national) and supposedly traditional) discourses on group security (Hansen and Nissenbaum 2009, 1160).

The complexity of the issue can be summarized in three kinds of threats (Ibid.) associated with this burgeoning field of security studies:

[5] Abdenur & Gama, 2015.

- Cybersecurity threats can be inflicted to the material facilities, which host digital properties, and through which those properties are played out by/to human users (Internet cables, ICT installations, hard drives, mainframes etc.). In this case it is usual to speak of *hardware* threats;

- Cybersecurity threats can stem *from* the system itself. Apart from the rare occurrence of systems explicitly designed to inflict harm on acknowledged (though non-authorized) users, such threats usually stem from the unpredictability of computers operating in different contexts and submitted to operational stress, engendering mechanical or digital malfunctioning. This provides a mix of *hardware* and *software* threats.

- Cybersecurity threats, finally, can work *through* otherwise benign systems by subverting the system's logic (that is where viruses, illegal data mining, phishing, wiretapping, cracking, hacking, piracy, malicious software, malware, adware in the case of cellphones get into the picture). In this case, we are speaking on *software* threats.

The novelty of cybersecurity in international relations did not mean technology was absent from the field. A myriad of terms indeed tried to cope with an expanding field of security in the early 1990s – even though hardly dealing with the issue of cybersecurity (Ibid., 1156):

"Yet, in spite of the widespread references to cyber insecurities in policy, media, and Computer Science discourses, there has been surprisingly little explicit discussion within Security Studies of what hyphenating ''security'' with ''cyber'' might imply. To take a recent example, the broadly conceived textbook, Contemporary Security Studies, edited by Alan Collins, has no entries for ''cyber security,'' ''computers,'' ''critical infrastructure,'' ''information security,'' or ''networks'' (Collins 2007). Those Security Studies scholars who do address cyber-related themes employ ''adjacent concepts''—'' cyber war'' (Der Derian 1992; Arquilla and Ronfeldt 1993), ''netwar'' and ''network security'' (Arquilla and Ronfeldt 1996, 2001; Deibert and Stein 2002; Der Derian 2003), ''critical infrastructure protection'' (Bendrath 2003), ''information security'' and ''information warfare'' (Denning 1999; Deibert 2003; Der Derian 2003:453; Latham 2003) — terms that overlap, but also have distinctive meanings that separate them from cyber security".

In the 21st century international relations are marked by normative diversity, with a decisive contribution stemming from emerging powers. Internet is a relatively new technology, having been set apart from digital inclusion for so long during Cold War (a reminder that ARPANET was designed to counter the USSR and potential US competitors). In a shifting international environmental, regulating the Internet and assuring cybersecurity entwined in decisive ways for countries that aspire to more than what they already have.

Emerging powers have had, for some time, their own Internet legislations (Brazil being the last, whose Marco Civil – Civilian Regulation of Internet Activities – considered the cutting edge of specialized legislation, reared its head in 2014 only).

South Africa has the Independent Communications Authority of South Africa (ICASA)[6], which since 1996, is in charge of regulating Internet intercourse (initially limited to e-mailing and overseeing provision)[7]. Legislation aimed for consumers' protection (2008) become, after the Snowden scandal, a Protection of Personal Information Act (2013).

India has long pushed for international regulation of Internet both in ITU and in the UN system. Domestically is exerts selective content control since the early 2000s (through the Information Technology Act, which was amended in more restrictive terms in 2008). Control mechanisms evolved to currently greater impacts on are "Internet intermediaries" in Indian legislation – any entity related to Internet services can be called upon by the Cyber Regulations Advisory Committee (on behalf of citizens, firms, civil organizations or the government) to remove control in a quick basis. India has also a Computer Emergency Response Team devised in 2004 to deal with cybersecurity threats.

As Russia's Internet use increased by leaps and bounds – from 8 million in 2001 to 65 in 2013 the government got more interested in regulating telecommunications at home. Anti-terrorist laws devised after the Chechen crisis of 1996 were joined by hosts of anti-piracy bills and attempts to curb political mobilizations (and to harass once again media oligarchs) during the second Vladimir Putin term. The legislation overlap implemented a *de facto* censorship on Internet content – much to the chagrin of the private sector, organized in film and television lobbies such as the Russian Association of Electronic Communications. On the other hand, non-government Internet-oriented organizations proliferate, such as the League of Safe Internet – whose activities (e.g., fighting child pornography) often provide context for the tightening of governmental grip on Internet activities.

China can be considered the most restrictive of emerging powers in terms of Internet access. The Beijing government, through the Steering Committee of the National People's Congress directly controls Internet provision, actively restricts content in order to curb political and religious contestations – which is often considered a threat to economic progress – and is currently attempting to build its own cable network "cut of" from the original US backbone. In 2010, the Chinese government defended such a matter on grounds of "Internet sovereignty" in its first white paper dedicated to this issue. At the same time, 300 million people use Chinese microblogs by conservative estimates and e-commerce have already become an asset of an increasingly interconnected Chinese economy. Internet traffic is, thus, a matter of great concern to Chinese authorities, not only in security terms, the sensitivity of which was enhanced by the Snowden scandal impinging on industrial secrets. That motivated a revival of the Chinese Law on Guarding State Secrets (now in a digital sense) and motivated the inception of 2014's Public Pledge on Self-*Regulation* and Professional Ethics for *China Internet* Industry, a legislation even more restrictive than the 2010 white paper[8]. At the same time, China pushes for Internet regulation at the international level; it even proposed, alongside India, that a specific UN organ be built for such a matter.

[6] https://www.icasa.org.za/

[7] http://ispa.org.za/spam/south-african-law/

[8] http://www.cfr.org/china/media-censorship-china/p11515

Emerging powers are considered as countries pushing the boundaries of the current architecture of international order. In terms of Internet regulation, much controversy lies with mix of increased government regulation and calls for international multilateralism. China, India, Russia and South Africa are considered by a non-governmental organization, OpenNet Initiative, countries that practice widespread Internet censorship[9] - an accusation that often translates as criticism of their democratic credentials. At the same time, those countries represent a considerable chunk of the world's Internet and cellphones users – as well as an even more pronounced contribution to emergent middle-classes, which are currently the major markets for such technologies. Internet and ITC are also strategic for emerging powers due to their economic multiplying effects. They comprise one of a few key areas able, according to the Brazilian government, to generate industrial spin-offs[10].

In this sense, it is expected that BRICS will invest their energies in regulating the Internet and in enhancing the national and international systems of cybersecurity – an issue that is increasingly featured in the declarations of BRICS Summits. However, it is still uncertain on whether they will achieve some sort of agreement of the approach through which this cooperation will take place. China and Russia seem more prone to inserting greater collaborations in cybercrime, security in ICTs and cyber terrorism as part of the agenda, while Brazil and India still remain reluctant.

Different normative settings across borders make for regulative abundance that may, nevertheless, eventually backfire. Differences between normative constellations can be employed by those who want to break the rules consistently. There is also a noticeable increase in complexity: shifting from different normative systems, interactions become more and more unpredictable. Those sovereign dilemmas were major drivers for the global governance debates of the early 1990s. Governance of the cyberspace poses, therefore, a twofold challenge. Firstly, governing the cyberspace deals with definitions, which are not currently shared across the globe. Secondly, as any realm of governance, it implicates the active collaboration of different social agents – with different agendas and investments. Governance cuts across sovereign borders and authority thresholds, in order to establish efficient social regulation.

Setting the Scene for International Cooperation

> *Presently, the international institutional architecture for the governance of cyberspace is dominated by a multiplicity of initiatives aimed at increasing cooperation at the international level as well as by the redefinition of the roles played by existent actors (Radu, 2013. p. 4)*

As said by Aristotle, human happenings in the world (actions) can assume a variety of forms. Some of them are endowed with causal powers (events). The entanglements of human happenings often make different actions overlap or clash. In such cases, we are dealing with problems of social action. Norms, in this sense, provide an arbitration for those inter-actions (Kratochwil, 1989). There are several pressures upon human

[9] https://opennet.net/research/regions
[10] http://www.sae.gov.br/site/wp-content/uploads/relatorio_XIIIENEE_ebook.pdf, p.23

actions, and norms provide a measure of stability and regulation: they define and guide.

Norms-building at the international stage comprises a lengthy process. Key issues are debated, negotiated, and sometimes resisted by different agents, states and otherwise (Abdenur & Gama 2015, pp. 456/457). Negotiations, proposals and implementation of international norms take place through a variety of area-specific institutions, including regimes (Krasner, 1983) and international organizations (Keohane, 1988). When the international agenda is broadened to encompass new issues, the process begins anew.

Normative shifts comprise interrelated problems (Kratochwil, 1989). There are norms that define something out of the universe of human happenings as a discrete realm of action, attributing particular features to it and defining, therefore, the social agency of that realm by allocating capacity for someone to act. This refers to constitutive norms (Onuf, 1989). In this constitutive dimension, we are dealing with how events fit in particular frames of activities deemed to be significant – categories, issue areas, regimes, functions, sectors (Abdenur & Gama 2015, p. 457). Once something has been framed out and defined, norms are put forth to regulate conduct within that realm — a set of rules of the game, which often includes an institutional setting projected to implement and monitor them, apart from other functions (Keohane, 1988).

Usually, in international relations what is considered an international event of unprecedented relevance ignites a new normative setting. After a new realm is defined, negotiations focus on the rules of the game and institutional design. In this sense, cybersecurity benefited from international experiences with norms-building.

Cybersecurity has now become theme of a yearlong list of international conferences and meetings. From January to December, these meetings and processes gather stakeholders from across the spectrum to discuss security in cyberspace. While this might indicate that cybersecurity has become an issue of international concern, one might question the effectiveness of these initiatives in advancing cooperation at the international level.

Attacks such as WannaCry, the Sony hacks, the Democratic National Committee hacks and the Mirai botnet have all made it to the headlines of newspapers and big media venues by highlighting the fragile state of security vis à vis the development of technologies and interconnected systems. As the theme gains traction in mainstream media, does this increased visibility of the impacts of cyber insecurity influence the course of international cybernorms?

Scholars have been mapping incidents (see Stoll, 1989; Healey et. al, 2013) and the continuous institutionalization of this evolving landscape (Portnoy and Goodman, 2009; Kuebris and Badiei, 2017; Nye, 2014). On one side, cybernorms literature emerges in the attempt to grasp the processes through which frameworks could be drawn in the attempt to accommodate the challenges for cultivating new norms and rules for cyberspace. “Norms offer a tool to coordinate action” (Finnemore, 2011. p.90), but what kinds of *norms* might be best suited to deal with the fast-paced change in cybersecurity? On the other, the discussion on cybernorms remains attached to state-to-state relations (Hurel and Lobato, 2017; Kuebris and Badiei, 2017)[iii]. How does the state-centric approach to cybersecurity impact the role of private companies, technical community and civil society's engagement in setting the norms?

In this regard, the definition of standards for appropriate behavior, capacity and confidence building measures have become the main mechanisms to responding to emerging threats in cyberspace (UNIDIR, 2017). By linking cybersecurity to traditional conceptions of international peace and security, – i.e. deterrence (Denning, 2016) – states seek to improve relations among them and guarantee greater predictability of undesirable actions. Recent developments in cybernorms include a continuous reference to the applicability International law, Law of Armed forces, dialogue within International forums and establishment of new initiatives. The overarching link to these efforts has been the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UNGGE) (Pawlak, 2016. p.130; Maurer, 2011).

In 2013 and 2015, the UNGGE got to the point where all states agreed on international law, whereas answering *how* international law would apply remained a the challenge for determining the future of cybernorms debate. The lack of "political appetite", as Spoerri puts it (see Parker, 2017), in reviewing and clarifying the applicability of international law in the prevention of conflict in cyberspace[iv] became clear as the UNGGE failed to reach a consensus a decade since its creation**.** Grigsby (2017. p.113-114) suggests that we have reached the "end of the road for norms" with the *roadblock* faced by the GGE in 2017. We argue that this is perhaps a *detour* on the road, where political appetite and agreements have shifted from international stalemate to bilateral cooperation.

This is gradual shift in course is highlighted by Former Cyber diplomat for the State Department, Chris Painter. He notes that the challenges permeating the development of cybernorms is not new, and it is less a question of whether this debate has matured, and more about the fact that of "some countries don't want to reach the conclusion of how international law applies to cyberspace". He added that the "next steps" would be to continue working with "like-minded countries around the world to pursue the affirmations of those [cybernorms, capacity and confidence building measures] norms and use them as the foundation for deterrence"[11].

While greater emphasis has been put to the shifting role of the US post-UNGGE failure (Grigsby, 2017), countries across different regions have sought to strengthen bilateral and regional cooperation on cybernorms and CBMs. The OAS in Latin America, ASEAN, and others have been promoting what might be referred to as the *turn* to like mindedness at the regional level (Pawlak, 2016. p.141-146) – and thus reflexively reinforcing the role of these forums as spaces for cooperation and consensus-building. This *shift* has been particularly significant in Southeast Asia. For example, Singapore's national Cyber Security Agency has established bilateral agreements with countries across almost all regions since 2015 – either on cybersecurity per se or on cybercrime.

[11] https://www.youtube.com/watch?v=1nybxZNgdZM

As Radu suggests, the proliferation of initiatives such as these call for a redefinition of the roles played by existent actors and that the complexity of the virtual environment plays out in the negotiation for its governance beyond technical assets, and thus in its global policy dimensions (Radu, 2013. p.4,10). As we saw in the previous sections, cybersecurity not only involves, but also relies on a multifaceted composition between actors, institutions, norms and initiatives; however, it has been emerging as a central concern in the political agenda of different countries (Hurel, 2016).

Alternative frameworks have emerged in the attempt to accommodate a less state-centric view on cybersecurity. According to ISOC's collaborative security approach, "everyone has the collective responsibility for the security of the Internet" and thus multistakeholder cross-border cooperation should be regarded as an essential component to the development of security in cyberspace. The approach outlines five pillars: preserving opportunities through confidence building, collective responsibility, fundamental properties and values, evolution and consensus, and think globally, act locally (Collaborative, 2015). ISOC's proposal can be associated to commons-based view of the Internet and upholds the development of mechanisms that are able to foster innovation, openness, collaboration, and shared-responsibility in cyberspace. This also includes user-centric views that understand cybersecurity as "the preservation – through policy, technology, and education – of the availability, confidentiality and integrity of information and its underlying infrastructure so as to enhance the security of persons both online and offline"[v].

The debate on Confidence Building Measures[vi] (CBM) also rises as a response to the consolidation of international cooperation in cybersecurity governance. Pawlak (2016. p.130) notes that the process of building confidence in cyberspace requires the involvement of all layers of society. Furthermore, Grigsby (2017) argues that the high level of skepticism with regards to the future of cybernorms can be taken forth by discussions on CBMs. However, there is no consensus on the scope and the objectives of these CBMs other than the shared conviction that they should respond to the lack of coordination and low levels of trust vis à vis growing participation of non-state actors in promoting insecurity. Some understand them as instruments of international politics aimed at preventing armed conflict and escalation through the establishment of preventive mechanisms between states (Ziolkowski, 2013). Nonetheless, recent reinterpretations have also included the need for a "multistakeholder-centric approach to leverage all possible stakeholders and to improve overall Internet resilience and decrease chances of miscalculation, mistrust, and misunderstanding"[vii] (Healey et al., 2013). Such reframing alludes to the recognition of the state as *part of* a wide variety of actors and reinforces the unfitting character of traditional state-centered CBMs (Healey et al., 2013).

Within this diverse call for institutions and norms, ICT companies have also been proactively engaging in shaping international policies. Microsoft has been one of the pioneers from the private sector in joining a global call for international norms for cyberspace. Two of the quintessential concerns set out by the company links to (i) the increasing role of states in regulating and interacting within cyberspace and (ii) the need for a multistakeholder approach for cybersecurity (International, 2014). This approach focuses in regulating state behavior in cyberspace and devising an international framework to hold heighten the stakes for states to engage in offensive behavior. Most of the concerns outlined in the proposals are directly related to state-centric views of cyberspace as an operational and warfare domain where strategies are played out in offensive and defensive moves. Microsoft has also argued that state attempts to bolster security through military focus could be harmful for innovation and stability of economic interests and developments (International, 2014).

In this field of positions, and position-takings, not only has the company been engaging with other initiatives at the international level — i.e.: Global Commission on the Stability of Cyberspace (GCSC) —, but investing in closer interaction with national governments in providing both technical and policy assistance[viii]. Moreover, by combining the international call for norms[ix] and the engagement with governments on the field of cybersecurity, the call for a Digital Geneva Convention[x] further strengthens the role of the company as international norms entrepreneurs[xi] for cybersecurity governance (Hurel and Lobato, 2017). This does not mean that the field of cybersecurity is "more crowded" — private companies have continuously been present in the regulation and development of the Internet (IGF, 2016) —, but it does indicate that current state-centric approaches to cybersecurity governance might be, left by itself, insufficient in attending to the range of stakeholders that are in fact impacted by vulnerabilities and attacks.

Thus, the *turn* in cybersecurity norms, as depicted above, results from issues such as the lack of representativeness in international fora and rising skepticism with regards to the effectiveness of international cooperation for cybersecurity. Furthermore, this *turn* has also been characterized by a push towards an epistemological shift in thinking about security – one that is presents a plethora of actors as part of the cybersecurity governance ecosystem, as well as both active agents and subjects to the implications of vulnerabilities. Notwithstanding, the examples outlined illustrate both the (i) proliferation of initiatives aimed at promoting some kind of governance and/or cooperative framework in the field of cybersecurity and (ii) the different institutional configurations that have emerged in the attempt to do so. Even though they are far from accounting the totality of the numerous organizations, institutions and initiatives that compose this playing field, they help us in understanding the specific configurations of actors and normative frameworks.

Final Remarks

From the onset, some questions pose considerable problems for matters of governing cyberspace in order to curb (what will be considered as) violations. We reserved some of them for the final remarks – on terms of "what must be done" to achieve some measure of governance in the cyberspace and of "what have we done" up to now.

Firstly, we may agree with Shires and Smeets (2017) when they say "cyber" has become an omnipresent term at the cost of its meaningfulness. It is a complex term that has reached a point where one must be cautious in using at as it refers to everything and nothing. However, when attached to "security", lines get more blurred (Hurel, 2016). In modalities of securitization, norms are only infrequently defined in multi-sectorial terms (Buzan, 1991). Security is usually framed as something unlikely to be *shared*. In this realm, sovereignty proved more than resilient. In terms of norms-building, we see a limiting grammar at work in in cyber**security** (emphasis placed). A new approach to security is (at least, tangentially) needed before we can meaningfully speak of governing cyberspace in order to foster security issues.

When security issues are at stake, usually a normative center is privileged, instead of contingent networks of different agents. The idea of security as a social good that takes precedence over the remainder (something that provides the core of securitization theories, according to Buzan) make even less plausible the constitution of a global institutional architecture to curb cybersecurity threats.

How does the state-centric approach to cybersecurity impact the role of private companies, technical community and civil society's engagement in setting the norms? *It* might still be of some use, in the sense that bilateral agreements are establishing safety networks among states and guidelines for their behavior. Although it might be unsustainable on the long run; if these agreements are not coupled with more representative bodies/initiatives at the national, regional and international level this will lead to further the structuration (Giddens, 1984) of shared understandings and cybernorms processes – in a scenario of security fragmentation (Hurel, 2016).

By shifting security issues from states to users, the governance of cyberspace arrives at another dead-end street. Getting rid of a single normative center implicates that a single cybersecurity regime may not fit the bill, even if it eventually make states' expectations converge (as predicted by Krasner and Keohane). In this sense, the idea of regimes is somehow inadequate, if they cannot incorporate a recursive dimension that builds upon a learning process among users (an old idea in international relations, which provided a lynchpin to functionalist theories since 1930s – see Mitrany, 1946). The notion of epistemic communities (Haas, 1992) provides a more nuanced account of complexities at work in collaboration based on shared learning in normative terms. – precisely, what the governance of cyberspace should attain, sometime in the future.

By narrowing down cybersecurity as part of the research agenda and as a way forward in international cybernorms discussion, we arrive at demands of a different order.

As a realm of practices, the cyberspace should provide its social agents some predictability. They should have more than a passing glimpse of roles and responsibilities. International relations was all but prepared for such a complex world. It was deeper and broader than what Keohane & Nye (1975) depicted in terms of complex interdependence, cutting across geographical lines and private-public ones.

As we stated previously, this is not a tabula rasa world – on the contrary, there are lots of norms in place. In such a world, private agents take the upper hand next to sovereigns. If the states depend on national legislations and on the United Nations and other institutions to find a compass across different national legislations, private firms boast their own regulations, and rank among the first to manifest interest in rendering the cyberspace more predictable. If states depend on International Law to do so, a mix of private regulation and gentlemen's agreements take place elsewhere. If the UN privileges what states let it see, other visions proliferate.

As the theme gains traction in mainstream media, does this increased visibility of the impacts of cyber insecurity influence the course of international cybernorms? Yes, as it has influenced as served as a platform for Microsoft, for example, to propose a Digital Geneva Convention. However (and not surprisingly), states have been shifting from international to bilateral agreements.

However, this scenario counters the most optimistic expectations of governance in the making. A proliferation of private clubs and bilateral agreements enhance complexity and uncertainty at the global level. At the same time, other norms (associated with the UN, such as multilateralism – Ruggie, 1992) get thinner and less cogent, adding fuel to systemic shortcomings.

Other nuances, more pronounced in cyberspace than elsewhere, also render normative attempts less effective. The kinds of norms that international agents usually deal with regulate the effects of human activities, at different temporalities – but those hardly cope with the kind of pace and variety endogenous of technological innovation in computer sciences. The lengthy processes of norms making at the international stage only duly fit innovation-friendly algorithms.

Taking into consideration the role of private agents and the pace of social innovation, we consider the following as signposts on the way of governing cyberspace:

a) International initiatives could benefit from the cumulative processes of common law;

b) The kinds of norms proposed shall be timely updated (in short span of time);

c) Private ordering shall be seriously considered. Recursive algorithms generate economies of scale, which enhances the appeal of expanding cybersecurity platforms or models. It be bring together states and firms, to some extent.

Bibliography

Barnett, M.N. & Finnemore, M. Rules for the World. London: Cambridge University Press, 2000.

Buzan, B. People, States and Fear – An Agenda for International Security Studies in the Post-Cold War Era. Essex: ECPR Press, 2nd edition, 1991

Collaborative (2015), "Collaborative Security: An approach to tackling Internet Security issues", available at: https://www.internetsociety.org/sites/default/files/Collaborative-Security.pdf

Denning, Dorothy (2016). Cybersecurity's Next Phase: Cyberdeterrence. Scientific American. Available at: https://www.scientificamerican.com/article/cybersecuritys-next-phase-cyber-deterrence/

Finnemore, M. and Sikkink, K. (1998). "International norm dynamics and political change". *International Organization*, 52 (4) : 887-917.

____________, and Hollis, D. B. (2016), "Constructing Norms for Global Cybersecurity", *American Journal of International Law*, Vol.110 No.3, pp. 425-479.

Giddens, A. The Constitution of Society. Cambridge: Polity, 1984.

Haas, E.B. Beyond the nation-state: Functionalism and international organization. Stanford: Stanford University Press, 1964.

Healey, J. (2013), "A Fierce Domain: Conflict in Cyberspace, 1986 to 2012". Cyber Conflict Studies Association, Arlington, VA.

________, Mallery, J. C., Jordan, K. T., and Youd, N. V. (2014), "Confidence Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security", available at: http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf

________, Mallery, J. C., Jordan, K. T., and Youd, N. V. (2014), "Confidence Building Measures in Cyberspace: A Multistakeholder Approach for Stability and Security", available at: http://www.atlanticcouncil.org/images/publications/Confidence-Building_Measures_in_Cyberspace.pdf

Hurel, L. M. (2016), "Cybersecurity and Internet Governance: Two Competing Fields(?)", Institute of International Relations, Pontifícia Universidade Católica do Rio de Janeiro (PUC-RJ). Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3036855

Hurel, L. M. and Lobato, L. (2017). Unpacking Cybernorms: Private Actors as Norms Entrepreneurs. Annual GigaNet Symposium.

IGF (2016), "IGF 2016 - day 3 - WK 2 - WS132 - NetGov, please meet Cybernorms. Opening the debate", available at: https://www.youtube.com/watch?v=dABnfGqN4hs

ITU – INTERNATIONAL TELECOMMUNICATION UNION. Measuring the Information Society Report 2013. Geneva: ONU, 2013

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

Keohane, R.O. & Nye Jr, J. Power and Interdependence: World Politics in Transition. Boston: Little, Brown, 1977.

Kobrin, S.J. (2001). Territoriality and the Governance of Cyberspace. Journal of International Business Studies, vol.32, no.4, pp.687-704.

Kuebris, Brenden and Badiei, Farzaneh (2017). Mapping the Cybersecurity Institutional Landscape. Digital Policy, Regulation and Governance.

Kurbalija, J.(2017), "Digital Geneva Convention: Multilateral treaty, Multistakeholder implementation", available at: https://www.diplomacy.edu/blog/digital-geneva-convention

Maurer, T (2011), "Cyber Norm Emergence at the United Nations — An Analysis of the UN's Activities Regarding Cyber-security", *Belfer Center for Science and International Relations*, Cambridge, MA. pp. 01-68.

http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

Nye Jr, J.S. & Keohane, R.O. Introduction. In: NYE JR., J.S. & DONAHUE, J. (eds). Governance in a Globalized World. Washington: Brookings Institution Press, p.1-21, 2000.

______ (2014). The Regime Complex for Managing Global Cyber Activities. Paper Series n. 1. CIGI.

Parker, Ben (2017). Bots and Bombs: Does Cyberspace need a "Digital Geneva Convention"? IRIN. Available at: https://www.irinnews.org/analysis/2017/11/15/bots-and-bombs-does-cyberspace-need-digital-geneva-convention

Pawlak, P. (2016). Confidence-Building Measures in Cyberspace: Current Debates and Trends. In. Osula, A. and Rõigas, H. International Cyber Norms: Legal, Policy and Industry Perspectives. NATO CCD COE. Tallinn.

Portnoy, M., and Goodman, S. (2009), "Global Initiatives to Secure Cyberspace: An Emerging Landscape", Springer Science and Business Media.

Radu, R. (2013), "Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace", in Kremer, J., and Müller, B. (Ed.) *Cyberspace and International Relations: Theory, Prospects and Challenges,* Springer, London, UK, pp. 3-20.

Robinson, P. (1999). The CNN effect: can the news media drive foreign policy? Review of International Studies 25, pp.301-309

Rosenau, J.N. (1990). Turbulence in World Politics*:* A Theory of Change and Continuity. *Princeton: Princeton University Press*

RUGGIE, J.G. Multilateralism matters – The theory and praxis of an institutional form. Columbia: Columbia University Press, 1993.

Stoll, Clifford 1989. The Cuckoo's Egg. New York: Doubleday.

Townes-Whitley, T. (2016a), "Addressing Cybersecurity and Transparency in Asia-Pacific with a Joint Transparency Center and Cybersecurity Center" available at: https://enterprise.microsoft.com/toni-townes-whitley/2016/10/03/asia-pacific-joint-transparency-cybersecurity-center/

_______________ (2016b), "The Trend Toward Transparency: Announcing the Microsoft Transparency Center in Brasilia", available at: https://enterprise.microsoft.com/toni-townes-whitley/2016/10/19/announcing-microsoft-transparency-center-brasilia/

UNIDIR (2017). The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century. United Nations Institute for Disarmament Research. Available at: http://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf

Ziolkowski, K. (2013), "Confidence Building Measures for Cyberspace — Legal Implications", available at: https://ccdcoe.org/publications/CBMs.pdf

[i] Louise Marie Hurel is a cybersecurity and Internet governance researcher. MSc candidate in Media and Communications (Data and Society) at the London School of Economics; holds a BA in International Relations from PUC-Rio. Researcher at the Brazilian Naval War College (NAC-EGN) and coordinator of the project "Cybersecurity and Digital Liberties" at Igarapé Institute think tank.

[ii] Carlos Frederico Pereira da Silva Gama is Director of International Affairs and lecturer of International Relations at the Federal University of Tocantins (UFT, Brazil).

[iii] Scholarly literature on norms development within International Relations has mostly focused in states and transnational advocacy networks (Finnemore and Sikkink, 1998; Keck and Sikkink, 1998) and that is perhaps one of the challenges that has been incorporated into the cybernorms discussion.

[iv] Philip Spoerri, representative of the International Committee of the Red Cross "said there may be value in clarifying other parts of international law about actions that don't meet the threshold of armed conflict, but noted that political appetite seemed lacking" (see Parker, 2017).

[v] See Freedom Online Coalition's definition of cybersecuirty at: https://freeandsecure.online/definition/

[vi] According to Ziolkowski (2013. p.5)"Confidence-building measures (CBMs) are an instrument of international politics, negotiated by and applied between states to strengthen international peace and security by reducing and eliminating the causes of mistrust, fear, misunderstanding, and miscalculations that states have about the military activities of other states."

[vii] Healey et al. (2014) propose that CBMs are divided into at least four types: collaborative, crisis management, restraint and engagement.

[viii] Microsoft has been continuously cooperating with governments, more specifically with several different countries in Latin America, Europe, Singapore and China in building what they have called *Transparency and Cybersecurity Centers*. Their main argument is that these centers are established in aiming at achieving UN's sustainable development goals (SDGs) — mainly goal 16: Peace, Justice and Strong Institutions (Townes-Whitley, 2016a, 2016b).

[ix] See Nicholas, 2014.

[x] In February 2017, Microsoft's CEO Brad Smith called for a Digital Geneva Convention. Building on the purpose of the Geneva Conventions, the proposal aimed at committing governments to protecting civilians and companies — from private-sector and critical infrastructure targeting — from nation-state attacks in times of peace (Kurbalija, 2017).

[xi] see Finnemore and Sikkink (1998. p.895) ; Also see Finnemore and Hollis, 2016 p. 446.