INSTITUTO IGARAPÉ
a think and do tank

STRATEGIC
NOTE
30
SEPTEMBER 2018

A Strategy for Cybersecurity Governance in Brazil

Louise Marie Hurel and Luisa Cruz Lobato

Index

A Strategy for Cybersecurity Governance in Brazil

Series:
Cybersecurity and Digital Liberties

Louise Marie Hurel and Luisa Cruz Lobato

Abstract

This study explores the institutionalization of the cybersecurity agenda in Brazil and seeks to identify opportunities for multi-stakeholder cooperation. It analyzes the key moments and processes that marked the development of the country's current cybersecurity architecture, highlighting the tensions which arose with the introduction of the agenda as a national security priority. The description of the cybersecurity governance ecosystem in Brazil opens up new avenues for the identification of solid opportunities for cooperation between different sectors inherently involved in the construction of this agenda -- as much in the technical field (cryptography and incident response) as in the elaboration of legislation, policies, and awareness campaigns.

Abbreviations

ABIN - Brazilian Intelligence Agency

APF - Federal Public Administration

CCSDCiber - Cybersecurity and Defense Coordination Center

CDCiber - Cyber Defense Center

CERT.br - Brazilian National Computer Emergency Response Team

CGI.br - Brazilian Internet Steering Committee

ComDCiber - Cyber Defense Command

CPI - Parliamentary Investigation Commission

CSIRT - Computer Security Incident Response Teams

CTIR.gov - Brazilian Computer Security and Incident Response Center

DNS - Domain Names System

DSIC-GSI - Department of Information and Communication Security

END - National Defense Strategy

GSI-PR - Institutional Security Cabinet

IoT - Internet of Things

MD - Ministry of Defense

NIC.br - Brazilian Network Information Center

PF - Federal Police

1. Introduction

Over the last decade, cybersecurity has been progressively institutionalized in Brazil. This process was concentrated in the actions of different sectors within the Federal Public Administration (APF), with the areas of defense and national security at its epicenter. The National Defense Strategy (END), of 2008, was the first official document to recognize cyberspace as one of the strategic domains for national security and defense — thus marking the official inclusion of cybersecurity into the national security agenda the insertion of cybersecurity into the national agenda.

This study identifies the key challenges and opportunities for cooperation in cybersecurity governance in Brazil. It argues that the elaboration of policies and directives in this area is not only a question of national security or defense. Rather, it is part of a broad governance process, which encompasses formal and informal cooperative arrangements between the different actors which compose the structure of Brazilian cybersecurity. This approach, founded on the processes that make up this governance ecosystem, sheds light on other possibilities for collaboration between sectors which are rarely taken into account from a more rigid structure characterized by sets of competencies (cybersecurity, information security, and cyber defense).

The main results were:

- The institutionalization of cybersecurity in Brazil was catalyzed by two main events. The first was the approval of the Marco Civil da Internet (the Digital Bill of Rights) in 2013, motivated by the political impact of the revelations regarding the United States' virtual surveillance structure. The second was a direct consequence of the mega-events hosted by the country between 2012 and 2016, which included efforts such as (i) the creation of the Cyber Defense Center (CDCiber); (ii) cybersecurity capacity building efforts by public institutions on the federal and municipal levels; (iii) the increased collaboration between the government and private sector; and (iv) the establishment of doctrines, policies, and directives related to cybersecurity.

- We identified at least our major effects resulting from the accelerated institutionalization process and the mega events in Brazil, that is: (i) the excessive securitization and accentuated militarization of cybersecurity; (ii) the exclusion of non-state actors from the definition of terms relevant to the political agenda; (iii) the ever-greater preference for solutions which seek to block applications, remove content; and (iv) the continuous difficulty of coordinating action at the level of the Federal Public Administration.

- These effects have equally impacted the formulation cybersecurity policy, with emphasis on: (i) tensions between prohibitionist, criminalization strategies and rights-based approaches; (ii) lack of collaboration between government actors, the private sector, civil society, and academics in policy development; and (iii) the absence of efficient mechanisms for collaboration and cybersecurity governance in the country.

- The major challenge for multi-stakeholder cybersecurity governance consists of a better definition of the roles and responsibilities for each sector. The visible lack of consensus and coordination hinders the sustainability of present and future policies.

The findings above indicate that, in order to overcome these challenges, it is fundamental to engage in the effort of identifying the potential areas of common interest (and/or operational overlap) and spaces for sectors to build trust among themselves. Therefore, the consolidation of a coherent structure of cybersecurity governance facilitates the identification and sharing of best practices, as well as stimulates increased coordination between sectors, which is necessary for responding to the growing challenges to the security, stability, and resilience of networks.

The strategic paper is divided in three parts. The first addresses the development of the current architecture of cybersecurity governance in Brazil, and offers a panorama of the main institutions engaged in this process. The second describes the operational and practical challenges to cooperation in the field during the cycle of mega-events hosted by the country between 2012 and 2016, as well as its effects on the accelerated development of the Federal Public Administration's (APF) internal structures. The final part presents recommendations for advancing cooperation between sectors. The methods adopted by the study include the mapping of institutions related to the structure of cybersecurity governance in the country and the organization of a focus group composed of technical specialists and representatives of government sectors, academia, civil society, and the private sector.

2. Structure of Governance and Institutions

Growing concerns with the capacity to respond and with the country's (in)capacity to fight them. However, increased diversification in methods and threats serves only as a partial response to the exponential growth of incidents in Brazil since 2011.[1] TThe projection of Brazil alongside major powers fighting cyberthreats in the context of mega-events coupled with the increasing exposure of national systems were key triggers for national cyber policy development.

Here we highlight two processes that can be considered fundemental traits to the build-up of a national governance ecosystem: (i) a spike on the creation of new institutions[2] dedicated to technical, strategic, and/or operational issues specific to this area; and (ii) the reorientation of already existing institutions,[3] which began to include aspects of cybersecurity[4] and network surveillance[5] in their list of activities and responsibilities.

The first step towards the consolidation of this governance structure (and the institutions therein) took place in the late 1990s — in the context of the creation of the Ministry of Defense (MD) and strengthening of national defense capabilities.[6] During the same period, the Ministry also launched its first information security policy and began setting new specialized agencies within the Federal Public Administration (APF). This includes, for example, the Center for Research and Development of Secure Communications (CEPESC), integrating the structure of the Brazilian Intelligence Agency.[7]

At a second stage, new spaces of cooperation and coordination between technical and defense sectors came into place in the period of the mega-events hosted by the country between 2012 and 2016. In this context, issues related to national security, defense, and threats, such as cyberterrorism and critical infrastructure, were prioritized by the AFP, fueling the development of policies and strategies in the area.

1 CERT.br (2018).

2 Such as CERT.br, CIRT.gov, CDCiber, ComDCiber, and others.

3 Such as the Federal Police or ABIN.

4 EXÉRCITO (2016).

5 MUGGAH; THOMPSON (2016).

6 ABDENUR (2014).

7 BRASIL (2000).

2.1. Restructuring the defense sector and establishing ant information security policy

The boom of the commercial Internet in 1993 (World Wide Web) meant that interconnectivity was no longer restricted to academic networks. It rapidly scaled into a global network, including Brazil.[8] In this context, the creation of the Brazilian Internet Steering Committee (CGI.br), in 1995, favored the development of policies vis à vis growing social and economic reliability on the Internet, established a multistakeholder structure for discussing national Internet developments, and consolidated new supporting institutions pertaining to this governance ecosystem.

Two agencies were established in the wake of security concerns derived from the rapid expansion of the commercial Internet and the operational infrastructure needed to maintain it. First, the Brazilian National Computer Emergency Response Team (CERT.br.)[9] was established, in 1997, following a study commissioned by CGI.br that sought to establish a "coordinating body for network security".[10] Second, the Brazilian Network Information Center (NIC.br), created in 2003, was tasked with the responsibility to implement CGI.br decisions and, in 2005, it started to administer ".br" domain name registrations.

CERT.br has become the focal point for incident response and notification in the country. It organizes trainings and capacity building events for both technical and non-technical audiences (e.g.: government bodies) and produces educational resources for users on the risks and threats in networks (e.g.: botnets, malware, phishing, spam).

The end of the 1990s and the beginning of the 2000s marked the consolidation of concepts and competencies related to information security. These processes took the form of agencies and policies for Internet governance and network security. In 2000, under the auspices of the National Defense Council, the Information Security Policy and the Information Security Steering Committee (CGSI) were created. Both included the mandate to establish directives, principles, and objectives for the development of norms, national technologies, and the preparation of APF entities and agencies in the field of information security.[11]

8 See RNP (s.d.).

9 CERT.br was structured after preoccupations with the security risks associated with the opening and expansion of the commercial Internet. See: NIC (1996).

10 GOMIDA et al. (1996).

11 Idem, Ibidem

At the time, a hierarchical system was established for federal decision-making. This (still current) national information security governance architecture stems from the Presidency (at the strategic level) to the Federal Police (operational level) and and the Institutional Security Cabinet (GSI-PR) -- which provides assistance to the presidency on security and defense issues and coordinates intelligence gathering and information security activities through the Brazilian Intelligence Agency (ABIN).

Subordinate to the GSI-PR, the Department of Information and Communication Security (DSIC-GSI) is directly responsible for the coordination of cybersecurity actions, including the operation and maintenance of a Brazilian Computer Security and Incident Response Center (CTIR.gov).[12] However, it is important to note that the maintenance of network security is not only the responsibility of the GSI-PR, but also of actors within the intelligence system, such as the Federal Police, private businesses, network operators and Computer Security Incident Response Teams (CSIRTs).

During the same period, the Brazilian Network Information Center (NIC.br) - created in 2005 - became one of the key organizations coordinating different technical aspects of Internet governance, encompassing, along with CERT.br and Registro.br, the (i) responsibility for registering and maintaining the domain names ".br" and (ii) the definition and implementation of security standards in IP address distribution (see Annex 1). Thus, in addition to implementing CGI.br decisions, NIC.br also guarantees network security, resilience, and stability.

As we will see in the next section, those institutions oriented toward Internet governance and cybersecurity operationally overlap in terms of the response to cybersecurity incidents and attacks. Whilst these institutional developments have historically taken place in specific sectors of the Federal Public Administration (Ministry of Science, Technology, and Communications and the Ministry of Defense), they meet at the operational level through the establishment of new channels of cooperation.

To guarantee network security within the scope of APF, the Decree n. 5.772, of 2006, created the aforementioned Brazilian Computer Security and Incident Response Center (CTIR.gov). From this moment on, cyber incident response within APF began to be coordinated by CTIR.gov, an entity falling within the scope of the Department of Information and Communication Security at the Institutional Security Cabinet. The Center also operates as a point for technical cooperation between other entities within APF and throughout the national network of CSIRTs (see Annex 2). Concomitantly, the Ministry of Justice (MJ), established the Cyber Crime Repression Services within the Federal Police, and it was tasked with the prevention and investigation of attacks against critical systems and infrastructures from the federal government. While not an agency oriented toward cybersecurity and defense, the Federal Police operates more directly with combatting specific types of cybercrime of transnational character.[13]

12 CITR.gov (2011).

13 The Federal Police has the constitutional competency to investigate transnational crimes to which Brazil committed through international treaties, and direct or indirect crimes against the Federal Public Administration(Art. 144, Federal Constitution). Law n. 13.124/2015 broadens its competency to investigating crimes against banks and ATMs.

At the level of the Ministry of Defense, the National Defense Strategy (END) -- launched in 2008 and updated in 2012 -- recognizes cyberspace as the third strategic domain for national defense and security, alongside the nuclear and space sectors.[14] It sets the priorities for political and strategic cooperation among the armed forces, as well as assigns the coordination of programs related to national defence in cyberspace to the army.[15]

A couple of years later, in 2016, the Cyber Defense Command (ComDCiber) was established, and, most importantly, composed by representatives from all armed forces. The agency is currently responsible for "planning, guiding, and controlling the operative, doctrinal activities of development and preparation at the level of the Military Cyber Defense System."[16] ComDCiber is an operational command group which is based in the regimental structure of the Brazilian Army, together with the Joint Staff, headed by the Navy, and the Department of Management and Strategy, headed by the Air Force. In this sense, the creation of ComDCiber marks a greater integration among the Armed Forces, evidencing the strengthening of the capacities of the Cyber Defense Center (CDCiber), as envisaged in the 2012 revision of END.[17]

14 BRASIL (2008)

15 The National Defense Strategy of 2008 identified three strategic sectors for the country and attributed a corresponding sector to each force: in this way, the Army was responsible for the cyber sector, the Navy, the nuclear sector, and the Air Force, the space sector. In its 2012 update, the Strategy sought to strengthen the Cyber Defense Center so that it evolved into the current Cyber Defense Command.

16 MD (2017)

17 BRASIL (2015)

Figure 1. Structure of Cybersecurity Governance in Brazil

As described, the institutionalization of cybersecurity in the country encompasses technical government agencies, which contribute to the development of distinct - albeit intrinsically related - sets of policies, norms, and practices. Figure 1 provides an overview of the cybersecurity governance structure in Brazil and considers the participation of these different sectors. It allows us to identify the key stakeholder groups and themes related to this structure, showing also that cybersecurity is a shared concern among a vast range of actors, and that its governance should include broader collaboration between them in respect to the formulation of integrated policies.

What is seen in this universe of cybersecurity governance is a set of competencies related to different societal sectors which operate starting from or at the intersection of such competencies The distinction between cybersecurity, cyber defense, and information security presented in figure 1 is as much operational as thematic. However, it is important to emphasize that this is a didactic division and that, in practice, the three topics overlap. Information security is the broadest of the three, concerning the risks inherent

to information systems and all types of control (physical, technical, procedural, and personal). It frequently leads to defensive measures to ensure vulnerability mitigation and treatment. Cybersecurity, in turn, concerns a set of risks presented in and stemming from cyberspace, including aspects of information security. Finally, cyber defense encompasses the threats which could directly affect the national security of the Brazilian State, as well as threats deriving from state actors. It is the most specific of the three competencies.

Finally, note that the comprehension of the different terms (cybersecurity, cyber defense, and information security)[18] and the mapping of the interaction between different parts of this field are challenges that remain on the horizon of future policy developments.

The next section deepens the discussion regarding the accelerated institutionalization of cybersecurity at the level of the Ministry of Defense and identifies cooperative spaces which have arisen in the past years, with an emphasis on the cycle of mega-events.

2.2. Cycle of mega-events and consolidation of the cybersecurity and defense regime at the national level

In 2013, former US government contractor Edward Snowden revealed that Brazil was also a target of USA espionage. This particular moment coupled with the cycle of mega-events hosted by Brazil between 2012 and 2016, there was a burgeoning demand by the President of the Republic and the Ministry of Defense for stronger cybersecurity mechanisms, institutions, and policies.[19] Responses implemented after these episodes characterized a new phase in the development and institutionalization of the sector in the country. This phase was marked by an emphasis on threats to national security and by the structuring of a Military Cyber Defense System at the level of the Federal Public Administration. However, during the same period, initiatives of coordination between these technical agencies and institutions also gained space.

Events such as the United Nations Conference on Sustainable Development (Rio+20) (2012), World Youth Day (2013), the Confederations Cup (2013), the World Cup (2014), and the Olympics and Paralympics (2016), involved a series of coordinated efforts between the Brazilian National Computer Emergency Response Team (CERT. br), Computer Security Incident Response Teams (CSIRTs), and other agencies with competencies related to cybersecurity issues. Moreover, these events also brought a series of exceptional structures designed for the occasion.

18 Cepik, Canabarro and Borne argue that "different types of cyber incidents lack a clear conceptual demarcation. The semantic confusion which was established around these concepts is not only prejudicial to research, but also imposes challenges to the adoption of public policies related to cyberspace and the internet" (2014), p. 178. This challenge, identified in 2014, remains an obstacle to the advance and opening of the process of participation in elaborating policies. While a clearer perception of their respective competencies exists for each actor, this affirmation does not hold when concerning the relations between different entities.

19 MINISTÉRIO DA DEFESA (2014)

Still in 2011, the Special Secretary for Mega Events was created to promote greater integration between federal, state, and municipal agencies in the security field. In 2012[20], the MD established guidelines for their participation in planning activities for the temporary use of the armed forces for cybersecurity and defense in cities hosting international events. One of the developments on the technical and operational incident response side was the creation of the "Rio 2016 CSIRT" to attend to the security of the Olympics. It operated jointly with CDCiber, the Cybersecurity and Defense Coordination Center (CCSDCIBER), CTIR.gov, and CERT.br.

The intensive involvement of military agencies and institutions in the field of cybersecurity in this period marks a process of its "securitization".[21] At the same time, a series of cyber threats (e.g.: espionage, information leakage, malware, denial of service attacks) began to be framed as national security priorities. Cyberterrorism and the risks associated with critical infrastructure[22] (e.g.: hydroelectric dams, electricity towers, airport communication networks) were thus prioritized to the detriment of threats not directly related to national security.

This context was also marked by popular dissatisfaction preceding the 2014 World Cup and the 2016 Olympics, including action by hacktivist networks. For example, the group Anonymous, known for its politically motivated cyberattacks, targeted and compromised government websites,[23] which strengthened the process of securitization. Among the agencies involved in formulating and executing the response to these attacks were the Center for Cyber Monitoring ("Centro de Monitoramento Cibernético"), CDCiber, the armed forces, the Federal Police,[24] CERT.br, and CTIR.gov.[25] The latter pair are responsible for the notification and warning of public and private agencies.[26]

Furthermore, the creation of a Parliamentary Committee of Inquiry on Espionage ("CPI da Espionagem"), with the objective of "investigating the denunciation of the existence of a system of espionage, structured by the United States government",[27] strengthened the national security focused approach. The main result of this CPI was the launch, by the Department of Information and Communication Security (DSIC-GSI), of a "Strategy

20 Ministerial document n. 2.221 of 2012, Ministry of Defense.

21 CEPIK; CANABARRO; BORNE (2014); DINIZ; MUGGAH; GLENNY (2014); LOBATO; KENKEL (2015); HUREL (2018).

22 "Installations, services, and goods which, if interrupted or destroyed, would provoke serious social, economic, political, or international impact, or impact to national security" (GSI-PR, 2010)

23 R7 (2013)

24 ROHR (2012)

25 CERTs and CSIRTs generally operate through a collaborative system of security incident response. CERT.br, for example, is central to security incident notifications in Brazil. CSIRTS possess diverse compositions, which include "ad hoc" groups geared toward the local environment up to regional, national, and/or private groups (HUREL, 2018).

26 BRAUN (2012)

27 FERRAÇO (2014).

for Information and Communications Security and Cybersecurity for the Federal Public Administration 2015-2018".[28] Parallel to a greater concern with cyber threats to national security, both the CPI da Espionagem and the visibility given to the topic of cyber insecurities also facilitated the adoption of administrative measures dedicated to increasing network security.

By the end of the cycle of mega-events, the competency for the implementation of cybersecurity strategy and policy in the country was shared by the following organizations: (i) the National Defense Council, which coordinates defense policy and strategy on the national level; (ii) GSI-PR, which, through the Department of Information and Communication Security, is responsible for information and communication security actions within the sphere of the Federal Public Administration (APF); (iii) ABIN, tasked with intelligence activities and the development of systems and secure communications for APF; (iv) the armed forces, through ComDCiber and CDCiber, tasked with the coordination and integration of cyber defense efforts in the country; and (v) the Ministry of Justice, through the efforts of the Federal Police in investigating cyber crimes against the APF or related to material protected by international conventions which the country has committed to.

Beyond the sphere of the Federal Public Administration, it was observed that several academic and technical organizations - e.g., universities, CERTs, and CSIRTs - and private organizations - such as small and medium businesses, as well as large corporations from the technology sector - played significant role in cybersecurity governance in Brazil.

One can therefore observe that the consolidation of cybersecurity and defense at the national level results from a combination of factors. In first place, the attempts to promote greater coordination between distinct domestic institutions aimed at its governance. In second, the necessity of responding to the challenges presented by the mega-events which occurred in the country and by external threats.[29]

28 Portaria CDN n. 14, 11 May, 2015

29 HUREL (2018)

3. Main challenges to cooperation

As shown in the preceding sections, a fair amount of institutions handle cybersecurity and defense in the Federal Public Administration. For this reason, their actions often surpass the technical and operational domains, reaching the political and juridical levels. Such diversification raised both challenges and opportunities for cooperation and coordination within this sphere.

Following the consultations held throughout the project, four set of challenges deserve further emphasis: (i) the risk of securitization and militarization of cybersecurity; (ii) the risk of excluding non-state actors from its the definition of priorities to the elaboration and implementation of cyber security related policies; (iii) the ever greater preference for measures such as the blocking of applications, content removal, and criminalization of online behavior; and (iv) coordination problems within the sphere of the Federal Public Administration.

The first set of challenges shed light onto how the risk of "securitization"[30] and the potential "militarization" of the structure are rooted on the period of the mega-events in the country. At that time, the task of devising solutions for the various security problems was allocated to the military sector. As the creation of specialized agencies — connected with the armed forces — and the attribution and broadening of ABIN and Federal Police responsibilities show, efforts to deal with cyber (in)security concentrated on the expansion of the competencies of agencies within the military apparatus and State intelligence. In turn,these efforts have resulted in a greater allocation of time and resources to combating threats such as terrorism, industrial sabotage, and cyber warfare, and a strengthening of the State's "surveillance apparatus".[31]

Closely connected to the first set, the second set of challenges suggests that the absence of channels for including non-state actors in policy-making also derives from securitization and militarization processes, which have ultimately removed from the public debate those topics judged as strategic to national security. As a consequence, the elaboration of cybersecurity policies becomes more restricted to security and intelligence agencies. The treatment of and response to threats through a logic of securitization "rekindles the normative trade-off between security and the respect for fundamental freedoms and rights",[32] placing them at opposite poles, rather than facing them as principles which should be placed side by side in cybersecurity policy-

30 CEPIK; CANABARRO; BORNE (2014); DINIZ; MUGGAH; GLENNY (2014); LOBATO; KENKEL (2015); HUREL (2018).

31 The so-called State surveillance apparatus corresponds to the institutions dedicated to practices and the development of espionage systems and strategy, and domestic and external surveillance.

32 CEPIK; CANABARRO; BORNE (2014).

making processes.[33] Under such circumstances, representatives of academia and civil society[34] stressed the importance of including multistakeholderism to the elaboration of directives, the structuring of agencies related to the national cybersecurity regime, and the process of policy elaboration for the sector.[35]

The third set of challenges speaks to a tendency to respond to security issues through blocking, content removal, and criminalization. This became evident after the proposal of bill 215/15, also named "PL Espião", which authorized the blocking of applications and websites and proposed the criminalization of a series of conducts - including copyright violations and unauthorized accesses to computers and systems - as emphasized in the final report from the Cyber Crimes Parliamentary Investigation Committee (CPICiber). In addition to CPICiber, several judicial decisions held between 2015 and 2016 have determined the blocking of applications,[36] motivated by the difficulty or impossibility in accessing encrypted data on social networks and messaging applications. These episodes contributed to elevating the tension between, on the one side, approaches focused on the criminalization of conducts and, on the other, rights based approaches to the Internet.

The fourth set, pertaining coordination challenges at the level of Federal Public Administration, suggests a lack of effective governance mechanisms for information and communication security, cybersecurity, and critical information assets. This adds to a difficulty in adapting cyber and information security policies elaborated on a strategic level to the operational level -- which means that security directives and guidelines written by DSIC and GSI tend to be only partially implemented; -- and to the absence of a central agency in charge of the executive coordination, in a systemic and participative manner, of information security, cybersecurity, and critical information assets, and with a budget adequate to the size of the problem.[37]

In addition to these challenges, two other trends also deserve emphasis. First, in what concerns technical collaboration, the mega-events, have also brought challenges for joint action (between diverse agencies) for the protection and resilience of the networks. In this sense, information sharing between organizers, network and systems operators, and CSIRTs was fundamental to coordination efforts during the 2014 World Cup[38] and the 2016 Olympics.[39]

Second, at the same time, incident response within and between organizations guided

33 CEPIK; CANABARRO; BORNE (2014), p.181.

34 ARTIGO 19 (2016); LOBATO; KENKEL (2015); DINIZ; MUGGAH; GLENNY (2014).

35 ARTIGO 19 (2016); HUREL (2018).

36 ITS RIO (2016).

37 BRASIL (2015).

38 HOEPERS (2014).

39 EB (2016).

and potentially redefined relations between different regimes and structures within the Brazilian architecture of cyber governance during the events.[40] Incident response initiatives included the military structure of the CDCiber as well as the action of external partners, such as CERT.br, private businesses, and other Federal Public Administration agencies. For example, despite having limited access to information on actors involved in promoting cybersecurity, less hierarchical structures such as CERT.br have also led the preparation and collaboration of post-Rio+20.[41]

Cooperation during the mega-events sheds a more clarifying light onto the interdependency between the public and the private sectors, as well as civil society, in cybersecurity governance. Adequate response to security challenges in the field involve the creation of formal and informal spaces for dialogue to enable greater interaction between representatives from these sectors.[42]

4. Final considerations and recommendations

The analysis has shown that cybersecurity does not possess an exclusive space within the sphere of the Brazilian government and that different responsibilities are assigned to various actors from the government, the private sector, academia, and civil society. It also sought to identify the different groups and institutions engaged with the agenda, as well as how they act and the possibilities for (and challenges to) cooperation among them. It was shown that the cycle of mega-events and the US mass surveillance scandal both strengthened and accelerated the institutionalization of cybersecurity at the level of the Federal Public Administration and the Ministry of Defense, marked by a focus on the cybersecurity of the Brazilian state.

It was also observed that, in the context of cybersecurity governance, coordination between the actors is not necessarily linked to conventional regulatory mechanisms. Extraordinary contexts, such as mega-events, have also contributed to the promotion of points of contact and spaces for coordination and collaboration between different actors, especially through partnerships between technical, non-governmental organisms and

40 HUREL (2018).

41 Idem, Ibidem.

42 MANDARINO JÚNIOR; CANONGIA (2010).

the military sectors. This suggests that opportunities for cooperation and dialogue can occur in specific contexts and processes. It is fundamental, however, to make sure that these collaborative efforts survive these extraordinary periods, constituting a more lasting structure of governance.

Convening sessions organized throughout the project allowed for the identification of points of convergence which favor cooperation and dialogue, and which should be promoted for the advancement of cybersecurity governance in Brazil:

Promoting a participative and multi-sector structure of cybersecurity governance

Cybersecurity governance should comprise the agenda's technical, thematic, and conceptual complexity, and include the full ecosystem of actors engaged with it. The national framework for Internet governance, headed by the CGI.br, should serve as an example for the development and incorporation of principles such as transparency, multidisciplinarity, and the multistakeholder model itself. An effective governance system requires advancing both operationalization and harmonization between those initiatives which are still sectorized. The elaboration of a National Strategy for Information Security and the creation of an agency to implement and manage this strategy are recommended, as is the responsible use of social network analysis and monitoring for information gathering about the urban quotidian and and public security issues.

Enhancing academia and civil society participation in cyber and information security governance

Despite the possibilities for cooperation between technical organisms, it is necessary to establish channels for cooperation to assure full and effective citizen participation. It is important to improve general understanding regarding information security and data protection, and relate it to cybersecurity, avoiding interpretations that restrict the access of civil society groups and academia to its governance.

These groups should be continuously consulted and included in relevant decision-making processes. Beyond playing a fundamental role, as they guarantee the continuity of policies and advocate for rights based approaches to data protection, these actors also contribute to combatting disinformation and developing ethical standards for data collection and analysis. Moreover, they inform the debate and, at times, promote training programs and awareness campaigns related to online risks. In what concerns these risks, it is important to remain attentive to themes such as (i) assuring the integrity of political information; (ii) the protection of sensitive public and industrial information in the context of foreign espionage; (iii) mechanisms of production and reproduction, human or automated, of "fake news"; and (iv) disinformation campaigns on the web.

Encouraging technical cooperation for cybersecurity

The public and private sectors should advance cooperation in the technical area, such as in incident response and the development and operation of systems and security standards, such as data encryption. Brazilian National Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) should intensify collaboration with the public and private sectors to exchange information on cyber attacks and system vulnerabilities, as well as collaborate in training incident response teams. Public administration entities, in turn, should invest in partnerships with CERTs and CSIRTs to adopt best practices and foster "digital hygiene" for cybersecurity and systems maintenance in public institutions. The Union, states, and municipalities should, moreover, prioritize the implementation of existing security technologies on their webpages, and their computer systems should be regularly updated. States and municipalities should assure that the networks, systems, and devices used in the administration of the urban quotidian are fortified against cyber attacks. These same actors should guarantee that all data collected, compiled, and analyzed be treated in accordance to international standards for data protection and in respect to ethical standards regarding its use.

Elaborating legislation and regulatory goals

Proposals for legislation and regulation should be attentive to the principles established by the Digital Bill of Rights. Moreover, regulatory and normative mechanisms should be sufficiently flexible to accompany technological development instead of being developed after a specific technology.

Awareness, education, and combatting disinformation on the internet

The government should invest in educational and awareness campaigns regarding internet use, online dissemination of disinformation, and the security risks in which determined behaviors can incur. It is fundamental that the measures adopted do not result in violations of freedom of speech and other fundamental rights set out in the Federal Constitution and the Digital Bill of Rights. Moreover, it is also important to the government to partner with civil society to create new channels for dialogue and trust for an open debate on the different dimensions of cybersecurity, beyond national security and defense.

As such, it should include approaches centered on and dedicated to the protection of users and the dissemination of best practices online. Raising awareness of rights, crimes, and technical and institutional tools for dealing with cyber attacks and disinformation campaigns should be encouraged. Social media and platforms should

commit to revising algorithms that prioritize content and with its transparency, indicating, for example, when a content, independent of its nature, has been removed. The academic community, in turn, should collaborate with the construction of evidences that allow for the mapping of security situations and phenomena, as well as the conduction and dissemination of studies on the real impact of web phenomena.

Developing ethical standards for network monitoring

Entities from the public administration, private sector, academia, and civil society should develop ethical standards regarding research and practices for network analysis and monitoring, in order to avoid that this type of practice results in investigations directed at specific people and groups. Institutions and organizations dedicated to these practices should still observe the purpose of data collection: personal data collected for a specific end should not be used for an end that is distinct from the original one. Actors should also clarify the type of monitoring conducted and whether the investigation is about a problem -- that is, identifying people, their behaviors and/or objects, -- or of a broader phenomenon, such as an investigation into the reach of fake news. Considering that investigations of a phenomenon can lead to sensitive data collection, the information compiled should be protected against misuse. Those using network monitoring to this end should also establish secure parameters for data collection, such as data anonymization for the people involved and, whenever possible, to prefer the use of publicly available data.

The five areas above identified encompass potential levels of cooperation and dialogue and reflect common concerns among members of the private sector, civil society, and the government. They suggest that, despite the variety of actors and institutions, as well as their interests and priorities, it is possible to find contact points and opportunities for collaboration which allow for the construction and consolidation of an architecture of governance for cybersecurity which is coherent with the desires and possibilities of the different Brazilian sectors.

References

ABDENUR, A. (2014). “Brazil and cybersecurity in the aftermath of the Snowden revelations”. In: Dane, F. (ed.). International security: a European-South American dialogue. Rio de Janeiro: Konrad Adenauer Siftung, p. 229-283.

ARTIGO 19 (2016). Brasil: análise da estratégia de cibersegurança. Sao Paulo: Artigo 19.

BRASIL. Decreto n.° 3.505, DE 13 DE JUNHO DE 2000. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Brasília, 13 June 2000. Available at: <http://www.planalto.gov.br/ccivil_03/ decreto/d305.htm>. Accessed: 15 Apr. 2018.

_____. (2008). Estratégia Nacional de Defesa. Brasília: Ministério da Defesa.

_____. (2012). Política Cibernética de Defesa. Brasilia: Ministry of Defense.

_____. (2015). Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018. Brasilia: Institutional Security Cabinet.

BRAUN, D. (2012). Exército prepara defesa cibernética da Copa das Confederações. Available at: <http://g1.globo.com/tecnologia/noticia/2012/08/exercito-prepara- defesa-cibernetica-da-copa-das-confederacoes.html>. Accessed: 27 May. 2018.

CDCIBER (2014). CDCIBER: perspectivas em face da espionagem eletrônica. VIII Curso de Extensão em Defesa Nacional UNAMA. Available at: <https://www. defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cedn/viii_cedn/ cibercidviicedn.pdf>. Accessed: 5 Jun. 2018.

CEPIK, M.; CANABARRO, D. R.; BORNE, T. (2014). “A securitização do ciberespaço e o terrorismo: uma abordagem crítica”. In: SOUZA, A. M.; NASSER, R.M.; MORAES, R. F. (eds.). Do 11 de setembro de 2001 à guerra ao terror: re exões sobre o terrorismo no século XXI. Brasilia: IPEA, p. 161-186.

CERT.BR. (2018). Estatísticas dos incidentes reportados ao CERT.br. Available at: <https://www.cert.br/stats/incidentes/>. Accessed: 27 May. 2018.

CTIR.GOV. (2011). Sobre o CTIR Gov. Available at: <http://www.ctir.gov.br/sobre- CTIR-gov.html>. Accessed: 26 May. 2011.

DINIZ, G.; MUGGAH, R.; GLENNY, M. (2014). Deconstructing cybersecurity in Brazil: Threats and responses. Rio de Janeiro: Igarapé Institute, p. 3-32. (Strategic Paper 11).

EXÉRCITO Brasileiro (2016). Exército, Abin e CGI.br farão a defesa cibernética nas Olimpíadas Rio 2016. Escritório de Projetos do Exército Brasileiro. Available at: <http://www.epex.eb.mil.br/index.php/ultimas-noticias/220-exercito-abin-e-cgi-br- farao-a-defesa-cibernetica-nas-olimpiadas-rio-2016>. Accessed: 14 Apr. 2018.

GOMIDE, A. C.; PINHEIRO, C. A. C.; VAZQUEZ, P. A. M. (1996). Grupos de trabalho – documento GT-S: Rumo a criação de uma coordenadoria de segurança de redes na internet Brasil. NIC.BR. Available at: < http://www.nic.br/pagina/grupos-de- trabalho-documento-gt-s/169#5>. Accessed: 18 Apr. 2018.

HOEPERS, C. (2014). Desafios e lições aprendidas no tratamento de Incidentes em grandes eventos. CERT.br. Available at: < https://www.cert.br/docs/palestras/ certbr-forum-csirts2014-02.pdf >. Accessed 23 May. 2018.

HUREL, L. M. (2018). "Securitização e governança da Segurança Cibernética no Brasil". In: Horizonte presente: tecnologia e sociedade em debate. Belo Horizonte: Letramento.

ITS Rio (2016). Bloqueio do WhatsApp viola a Constituição e os direitos humanos. Instituto de Tecnologia e Sociedade do Rio. Available at: <https://feed. itsrio.org/bloqueio-do-whatsapp-viola-a-constitui%C3%A7%C3%A3o-e-os-direitos-humanos-aeaa0d94f2ae>. Accessed 17 Apr. 2018.

LOBATO, L. C.; KENKEL, K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. Revista brasileira de política internacional, Brasilia, v.n 58, n. 2, p. 23-43, Dez. Available at: <http://www.scielo. br/scielo.php?script=sci_=arttext&pid=S0034-73292015000200023&lng=en&nrm=iso>. Accessed: 18 Apr. 2018.

MANDARINO JUNIOR, R.; CANONGIA, C. (2010). Livro verde: Segurança Cibernética no Brasil. Brasilia: GSIPR/SE/DSIC.

MINISTÉRIO da Defesa (2014). "Ministro acompanha trabalho de defesa cibernética na Copa do Mundo." Ministério da Defesa. Available at: <http://www.defesa.gov. br/index.php/noticias/13141-ministro-acompanha-trabalho-de-defesa-cibernetica-na- copa-do-mundo>. Accessed: 22 Jul. 2018.

_____ (2017). Comando conjunto de defesa cibernética. Ministério da Defesa. Available at: <https://www.defesa.gov.br/noticias/30417-comando-conjunto-na- defesa-cibernetica>. Accessed: 02 Jun. 2018.

MUGGAH, R.; THOMPSON, N. B. (2016). Brazil must rebalance Its approach to cybersecurity. Council on Foreign Relations. Available at: <https://www.cfr.org/blog/brazil-must-rebalance-its-approach-cybersecurity> Accessed: 19 Apr. 2018.

NIC (1996). Rumo à criação de uma coordenadoria de segurança de redes na internet no Brasil. NIC.br. Available at: <http://www.nic.br/pagina/grupos-de- trabalho-documento-gt-s/169#4>. Accessed: 27 May. 2018.

R7 (2013). Anonymous invade site do governo para apoiar protesto do Movimento Passe Livre. Available at: <https://noticias.r7.com/sao-paulo/anonymous-invade- site-do-governo-para-apoiar-protesto-do-movimento-passe-livre-19062013>. Accessed 16 May. 2018.

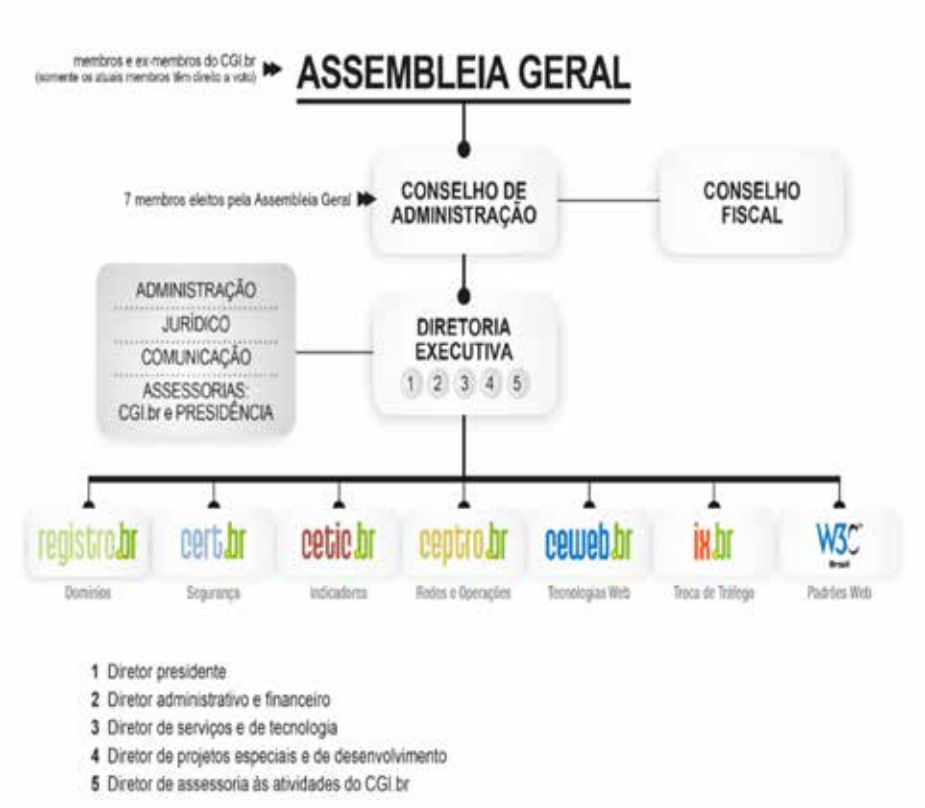
RNP (s.d.). A História por trás dos 20 anos da internet comercial no Brasil. Rede Nacional de Pesquisa. Available at: <https://www.rnp.br/destaques/historia-por- tras-20-anos-internet-comercial-brasil>. Accessed: 27 May. 2018.

ROHR, A. (2012). Anonymous ataca sites ligados ao governo em protesto contra a Rio+20. G1. Available at:<http://g1.globo.com/tecnologia/noticia/2012/06/ anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20. html>. Accessed: 27 May. 2018.

FERRAÇO, R. (2014). CPI da espionagem. Senado Federal. Available at: <https://www12.senado.leg.br/noticias/arquivos/2014/04/04/integra-do-relatorio-de-ferraco>. Accessed 02 Jun. 2018.

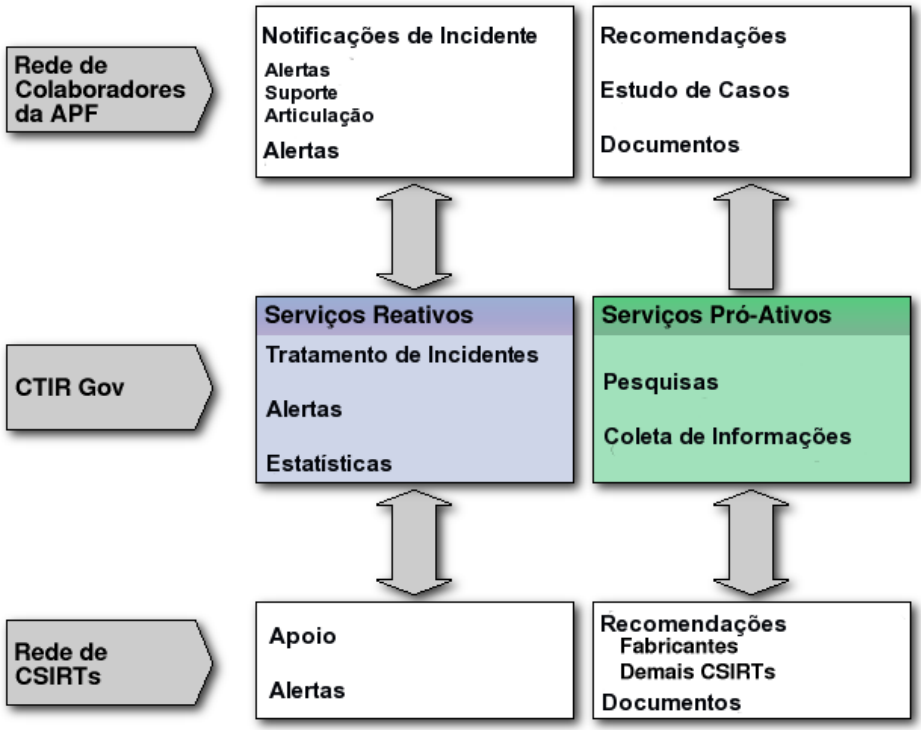
SOPRANA, P. (2016). Robert Muggah: O governo brasileiro não é inocente quando o assunto é espionagem. Época. Available at: <https://epoca.globo.com/vida/experiencias-digitais/noticia/2016/06/robert-muggah-o-governo-brasileiro-espionou-seus-cidadaos.html> Accessed: 17 Apr. 2018.

Annex 1: Structure of NIC.br



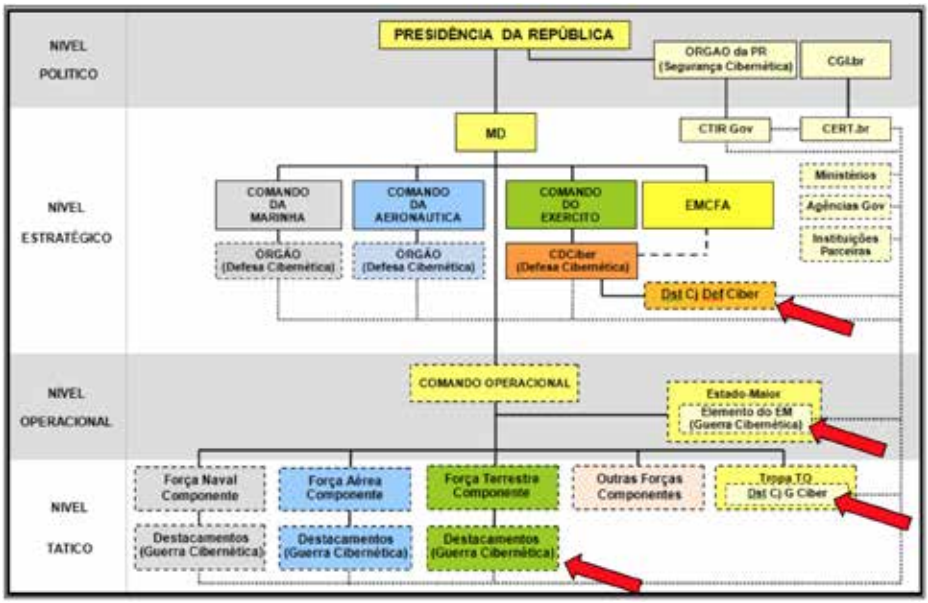
Font: NIC.br

Annex 2: Structure of Collaboration CTIR.gov



Font: CTIR.gov

Annex 3: Structure of Military Cyber Defense System



Font: CDCiber, 2014

About the Series

The series of strategic papers is part of the Igarapé Institute's Cybersecurity and Digital Liberties project, with support from Open Society Foundations (OSF). This project brings together a set of reflections, strategic papers and policy recommendations which aim to provide a critical reflection on the main challenges that permeate the relation between security, privacy, and the use of new technologies in Brazil. The strategic papers were developed by Igarapé's cybersecurity team and it is based on a series of dialogs organized between 2017 and 2018 with representatives from the private sector, government, civil society, technical community and academia. Seeking to encompass different readings and perspectives on the balance between criminalization approaches and the strengthening of rights (such as the right to privacy), the series also features articles from specialists analyzing the post-Digital Bill of Rights era in light of the introduction of the Internet of Things into the national agenda, and the approval of Brazil's first General Data Protection Regulation.

Other Igarapé Institute Publications

STRATEGIC PAPERS

STRATEGIC PAPER 34 - Colômbia e as FARC: cenários pós-conflito e repercussões regionais

Guilherme Damasceno Fonseca and Christian Vianna de Azevedo

(May 2018)

STRATEGIC PAPER 33 - Citizen security in Latin America: Facts and figures

Robert Muggah and Katherine Aguirre Tobón

(March 2018)

STRATEGIC PAPER 32 - A agenda sobre mulheres, paz e segurança no contexto latino-americano: desafios e oportunidades

Renata Avelar Giannini, Ana Paula Pellegrino, Carol Viviana Porto, Luisa Lobato, Maiara Folly and Mariana Gomes da Rocha

(March 2018)

STRATEGIC PAPER 31 - Implementando a agenda sobre “Mulheres, Paz e Segurança” no Brasil: uma revisão do Plano Nacional de Ação

Paula Drumond and Tamya Rebelo

(March 2018)

STRATEGIC PAPER 30 - A percepção de crianças e adolescentes sobre a segurança e a violência: a aplicação do Índice de Segurança da Criança em uma escola

Renata Avelar Giannini, Maiara Folly, Monica de Cassia Nehrebeck and Willian Vinícius Silva (May 2017)

STRATEGIC PAPER 29 - Migrantes invisíveis: a crise de deslocamento forçado no Brasil Maiara Folly (Março 2018)

STRATEGIC PAPER 28 - Salas de Consumo de Drogas: situando o debate no Brasil

Rafael Tobias de Freitas Alloni e Luiz Guilherme Mendes de Paiva (Outubro 2017)

STRATEGIC PAPER 27 - Situações extraordinárias: a entrada das mulheres na linha de frente das forças armadas

Renata Avelar Giannini, Maiara Folly, Mariana Fonseca Lima (Agosto 2017)

STRATEGIC PAPER 26 - A percepção de crianças e adolescentes sobre a segurança e a violência: a aplicação do Índice de Segurança da Criança em uma escola

Renata Avelar Giannini, Maiara Folly, Monica de Cassia Nehrebeck and Willian Vinícius Silva

(May 2017)

STRATEGIC PAPER 25 - Brazil, the internet and the Digital Bill of Rights reviewing the state of Brazilian internet governance

Daniel Arnaudo

(April 2017)

STRATEGIC PAPER 24 - Confiança em desenvolvimento: o Brasil e os projetos de impacto rápido

Eduarda Hamann, Henrique Garbino and Maiara Folly

(April 2017)

STRATEGIC PAPER 23 - Controlando el territorio y construyendo seguridad y justicia en el posconflicto colombiano. Edición especial de los Diálogos por la Seguridad Ciudadana

(December 2016)

STRATEGIC PAPER 22 - Durões contra os fracos; fracos frente aos durões: as leis de drogas e a prática da ação policial

Juan Carlos Garzón Vergara

(October 2016)

STRATEGIC PAPER 21 - Infância e Segurança: um estudo sobre a percepção da violência por crianças e adolescentes do Complexo do Muquiço, Rio de Janeiro

Renata A. Giannini, Maiara Folly, Victor Ladeira, Andressa Werneck and Renata Siqueira

(July 2016)

STRATEGIC PAPER 20 - Making cities safer: Citizen security innovations from Latin America

Robert Muggah, Ilona Szabo de Carvalho, Nathalie Alvarado, Lina Marmolejo and Ruddy Wang

(June 2016)

STRATEGIC PAPER 19 - Construindo Planos Nacionais de Ação eficazes: coletânea de boas práticas

Renata A. Giannini

(March 2016)

STRATEGIC PAPER 18 - "When kids call the shots" children's perceptions on violence in Recife, Brazil, as per the 'Child Security Index'

Helen Moestue, Katherine Aguirre and Renata A. Giannini

(December 2015)

STRATEGIC PAPER 17 - Where is Latin America? Reflections on peace, security, justice and governance in the Post-2015 Sustainable Development Agenda

Renata A. Giannini

(October 2015)

STRATEGIC PAPER 16 - Políticas de drogas no Brasil: a mudança já começou

Ilona Szabó de Carvalho and Ana Paula Pellegrino

(March 2015)

STRATEGIC PAPER 15 - Nuevos retos y nuevas concepciones de la seguridad en México Edición especial de los diálogos por la seguridad ciudadana

(March 2015)

STRATEGIC PAPER 14 - A 'third umpire' for policing in South Africa – applying body cameras in the Western Cape

David Bruce and Sean Tait

(March 2015)

STRATEGIC PAPER 13 - Brazil and Haiti: Reflections on 10 years of peacekeeping and the future of post-2016 cooperation

Eduarda Passarelli Hamann (org.)

(January 2015)

STRATEGIC PAPER 12 - Measurement matters: Designing new metrics for a drug policy that works

Robert Muggah, Katherine Aguirre and Ilona Szabó de Carvalho

(January 2015)

STRATEGIC PAPER 11 - Desconstruindo a segurança cibernética no Brasil: ameaças e respostas

Gustavo Diniz, Robert Muggah and Misha Glenny

(December 2014)

STRATEGIC PAPER 10 - Expansão Digital: como as novas tecnologias podem prevenir a violência contra crianças nos países do hemisfério sul

Helen Mostue and Robert Muggah

(November 2014)

STRATEGIC PAPER 9 - Promover gênero e consolidar a paz: a experiência brasileira

Renata A. Giannini

(September 2014)

STRATEGIC PAPER 8 - Tornando as cidades brasileiras mais seguras: edição especial dos diálogos de segurança cidadã

Michele dos Ramos, Robert Muggah, José Luiz Ratton, Clarissa Galvão, Michelle Fernandez, Claudio Beato, Andréa Maria Silveira, Melina Ingrid Risso and Robson Rodrigues

(July 2014)

STRATEGIC PAPER 7 - Changes in the neighborhood: Reviewing citizen security cooperation in Latin America

Robert Muggah and Ilona Szabó de Carvalho

(March 2014)

STRATEGIC PAPER 6 - Prevenindo a violência na América Latina por meio de novas tecnologias

Robert Muggah and Gustavo Diniz

(January 2014)

STRATEGIC PAPER 5 - Protegendo as fronteiras: o Brasil e sua estratégia "América do Sul como prioridade" contra o crime organizado transnacional

Robert Muggah and Gustavo Diniz

(October 2013)

STRATEGIC PAPER 4 - To save succeeding generations: UN Security Council reform and the protection of civilians

Conor Foley

(August 2013)

STRATEGIC PAPER 3 - Momento oportuno: revisão da capacidade brasileira para desdobrar especialistas civis em missões internacionais
Eduarda Passarelli Hamann
(January 2013)

STRATEGIC PAPER 2 - A fine balance: Mapping cyber (in)security in Latin America
Gustavo Diniz and Robert Muggah
(June 2012)

STRATEGIC PAPER 1 - Mecanismos nacionais de recrutamento, preparo e emprego de especialistas civis em missões internacionais
Eduarda Passarelli Hamann
(May 2012)

STRATEGIC NOTES

STRATEGIC NOTE 29 - Will Cuba update its drug policy for the twenty first century?
Isabella Bellezza-Smull
(Decembro 2017)

STRATEGIC NOTE 28 - Desafios e boas práticas para implementação da Agenda sobre Mulheres, Paz e Segurança
Renata Avelar Giannini and Maiara Folly
(November 2017)

STRATEGIC NOTE 27 - À margem do perigo: preparo de civis brasileiros para atuação em países instáveis
Eduarda Passarelli Hamann
(June 2017)

STRATEGIC NOTE 26 - Haitian women's experiences of recovery from Hurricane Matthew
Athena Kolbe, Marie Puccio, Sophonie M. Joseph, Robert Muggah and Alison Joersz
(June 2017)

STRATEGIC NOTE 25 - O futuro das operações de manutenção da paz das Nações Unidas: uma perspectiva brasileira (implementação do relatório HIPPO)
Eduarda Hamann and Adriana Erthal Abdenur
(March 2017)

STRATEGIC NOTE 24 - Em busca da igualdade de gênero: boas práticas para a implementação da agenda sobre mulheres, paz e segurança

Maiara Folly and Renata Avelar Giannini

(March 2017)

STRATEGIC NOTE 23 - Filling the accountability gap: principles and practices for implementing body cameras for law enforcement

Robert Muggah, Emile Badran, Bruno Siqueira and Justin Kosslyn

(November 2016)

STRATEGIC NOTE 22 - Latin American dialogue on international peace and security reviewing the prospects for peace operations, peacebuilding and women, peace and security (May 2016)

STRATEGIC NOTE 21 - Assessing Haiti's electoral legitimacy crisis – results of a 2016 survey

Athena R. Kolbe and Robert Muggah

(February 2016)

STRATEGIC NOTE 20 - Impact of perceived electoral fraud on haitian voter's beliefs about democracy

Athena R. Kolbe, Nicole I. Cesnales, Marie N. Puccio and Robert Muggah

(November 2015)

STRATEGIC NOTE 19 - A path forged over time: Brazil and the UN missions (1947-2015)

Eduarda Passarelli Hamann

(June 2016)

STRATEGIC NOTE 18 - Implementing UNSC resolution 1325 in Brazil: surmounting challenges and promoting equality

Renata A. Giannini, Mariana Lima and Pérola Pereira

(October 2015)

STRATEGIC NOTE 17 - A reforma do Conselho de Segurança da ONU: visão de mundo e narrativas do Brasil

Eduarda Passarelli Hamann

(May 2015)

STRATEGIC NOTE 16 - Break your bones: Mortality and morbidity associated with Haiti's Chikungunya epidemic

Athena R. Kolbe, Augusta Herman and Robert Muggah

(July 2014)

STRATEGIC NOTE 15 - New technologies for improving old public security challenges in Nairobi

Mads Frilander, Jamie Lundine, David Kutalek and Luchetu Likaka

(June 2014)

STRATEGIC NOTE 14 - O despertar da América Latina: uma revisão do novo debate sobre politica de drogas

Ilona Szabó de Carvalho

(February 2014)

STRATEGIC NOTE 13 - The changing face of technology use in pacified communities

Graham Denyer Willis, Robert Muggah, Justin Kossyln and Felipe Leusin

(February 2014)

STRATEGIC NOTE 12 - A inserção de civis brasileiros no sistema ONU: oportunidades e desafios

Renata Avelar Giannini

(January 2014)

STRATEGIC NOTE 11 - A diáspora criminal: o alastramento transnacional do crime organizado e as medidas para conter sua expansão

Juan Carlos Garzón Vergara

(November 2013)

STRATEGIC NOTE 10 - Smarter policing: tracking the influence of new information technology in Rio de Janeiro

Graham Denyer Willis, Robert Muggah, Justin Kosslyn and Felipe Leusin

(November 2013)

STRATEGIC NOTE 9 - Is tourism Haiti's magic bullet? An empirical treatment of Haiti's tourism potential

Athena R. Kolbe, Keely Brookes and Robert Muggah

(June 2013)

STRATEGIC NOTE 8 - Violencia, drogas y armas ¿Otro futuro posible?
Ilona Szabó de Carvalho, Juan Carlos Garzón and Robert Muggah
(July 2013)

STRATEGIC NOTE 7 - A promoção da paz no contexto pós-2015: o papel das potências emergentes
Robert Muggah, Ivan Campbell, Eduarda Hamann, Gustavo Diniz and Marina Motta
(February 2013)

STRATEGIC NOTE 6 - After the storm: Haiti's coming food crisis
Athena Kolbe, Marie Puccio and Robert Muggah
(December 2012)

STRATEGIC NOTE 5 - Brazil's experience in unstable Settings
Eduarda Passarelli Hamann and Iara Costa Leite
(November 2012)

STRATEGIC NOTE 4 - Cooperação técnica brasileira
Iara Costa Leite and Eduarda Passarelli Hamann
(September 2012)

STRATEGIC NOTE 3 - A Experiência do brasil em contextos instáveis
Eduarda Passarelli Hamann and Iara Costa Leite
(August 2012)

STRATEGIC NOTE 2 - The economic costs of violent crime in urban Haiti (Aug 2011 - Jul 2012)
Athena R. Kolbe, Robert Muggah and Marie N. Puccio
(August 2012)

STRATEGIC NOTE 1 - Haiti's urban crime wave? Results from monthly households surveys (Aug 2011 - Feb 2012)
Athena R. Kolbe and Robert Muggah
(March 2012)

IGARAPÉ INSTITUTE

a think and do tank

The Igarapé Institute is an independent think and do tank devoted to evidence-based policy and action on complex social challenges in Brazil, Latin America, and Africa. The Institute's goal is to stimulate debate, foster connections and trigger action to address security and development. Based in the South, the Igarapé Institute undertakes diagnostics, generates awareness, and designs solutions with public and private partners, often with the use of new technologies. Key areas of focus include citizen security, drug policy, cybersecurity, building peace and safer cities. The Institute is based in Rio de Janeiro, with personnel across Brazil, Colombia, Mexico and the United States. It is supported by bilateral agencies, foundations, international organizations and private donors.

Igarapé Institute
Botafogo, Rio de Janeiro – RJ – Brasil - 22281-000
Tel/Fax: +55 (21) 3496-2114
contato@igarape.org.br
facebook.com/institutoigarape
twitter.com/igarape_org

https://igarape.org.br/en/

Art direction
Raphael Durão - STORM.pt

ISSN 2359-0998

IGARAPÉ INSTITUTE

a think and do tank

www.igarape.org.br/en/