3-1-2013

Brazil and The Fog of (Cyber) War

Diego Rafael Canabarro
University of Massachusetts - Amherst

Thiago Borne

National Center for Digital Government

Brazil and The Fog of (Cyber)War

Diego Rafael Canabarro
PhD candidate in Political Science at the Federal University of Rio Grande do Sul (UFRGS)
Research assistant at the Center for International Studies on Government (CEGOV/UFRGS)
NCDG Fellow 2012-2013

and

Thiago Borne
PhD candidate in Strategic Studies at UFRGS
Research assistant at CEGOV/UFRGS

NCDG Policy Working Paper No. 13-002
Submitted March 1, 2013

INTRODUCTION

This paper furthers the analysis presented in the previous working paper, "Reflections on the Fog of (Cyber)War" (Canabarro & Borne, 2013), by assessing the Brazilian approach to cybersecurity. It analyses some of the most important documents on security issued by the Brazilian government since redemocratization in order to access the adequacy of its policy in the light of the controversies presented before. The paper first pictures cyberspace in Brazil and introduces three landmark documents that guide security policy towards it: the (a) National Strategy of Defense, the (b) White Paper to Guide Future Defense Priorities, and the (c) Green Book on Brazil's Cybersecurity. Finally, the paper presents some remarks on both the positive and negative aspects of the policy.

THE BRAZILIAN APPROACH TO CYBERSECURITY

Data retrieved from the Brazilian Center of Studies on Information and Communication Technologies (CETIC.br, 2011) reveal that figures vary a lot when it comes to the number of households[1] that possess ICTs (related or not to the Internet) in Brazil: TV sets (98%), cell phones (87%), radios (80%), fixed telephone lines (37%), PCs (36%), laptops (18%), satellite TV (52%), and videogames (22%). Only thirty-two percent (32%) of the households in Brazil have access to the Internet. Sixty-five percent (65%) of those connect to the Internet with speeds greater than 256 Kbps. Around fifty-three percent (53%) of the population has already accessed the Internet.[2] During the last surveyed year (2011-2012), thirty-one percent (31%) of the ones who had already accessed the Internet had used some sort of e-government service in order to acquire information (23%) and to perform *on line* transactions such as paying taxes, filling-in forms, and downloading software (11%). Twenty-nine percent (29%) of the Internet users in the country have already purchased goods and services through the Internet.[3]

Mobile technology has also spread on a fast track in the country, following a worldwide trend. (ITU, 2011) The Brazilian Agency for Telecommunications (ANATEL) reports that, by the end of 2012, around 260 million cell phones were operating in the country (more than 1,3 line *per capita*).

Up to the 1990s, the telecom market in Brazil was largely monopolized by the public sector. Liberal policies adopted in the mid-1990s[4] led the government to transfer its assets to the private sector through a process of privatization, and the Federal Government became a mere regulator of the telecom market. (Miranda, Kune & Piani, 2011)

With telecom liberalization, coupled with the commercialization Internet access in the turn of the century, a myriad of service providers of all sorts entered the stage. Today, private foreign and domestic companies (such as Telefónica/Vivo, Claro Américas/Claro, Embratel/Oi, etc.) own the largest part of the infrastructural backbone of telecom networks. Most notably, the cables for the connection of Brazil's domestic networks to the ones located abroad are property of the formerly

[1] The last census carried out in Brazil (2010) estimates that the country has a population of over 190 million people living in 67,5 million households. For more information, see the website of the Brazilian Census Bureau (IBGE) on: http://www.ibge.gov.br/english/. Last accessed: 12/13/2012.

[2] From 2005 to 2011, the pool of Internet in Brazil users grew from 32% to the current 53%.At home, at work, at school, at a friend's house, at an Internet café or Telecenter, and through a cell phone. The most common applications are: e-mails exchange (78%), social networking (69%), blogging, twitting, and creating webpages in general (37%).

[3] Among the top-three reasons for not interacting with governmental agencies and online stores are: the need of having interpersonal contact, security/privacy issues, and difficulties for using the services (especially e-government).

[4] The country abided by the tenets of the goods and services trade liberalization advanced within the World Trade Organization. (Schiller, 1999; Drake, 2008)

government-owned Embratel, currently an open-capital company controlled by *Forbes Magazine* number one billionaire of 2012, Carlos Slim Helú from Mexico.

Governments in the federal, state, and municipal levels maintain exclusive networks for different purposes (finances, health care, education, transportation, law enforcement and security, defense, etc.), and with different levels of interconnectivity among themselves and with other privately-owned networks.[5]

That is just a summarized snapshot of part[6] of the Brazilian cyberspace. It does not include, for example, the (foreign) satellite networks used in the country, dedicated lines of communication used by the private sector, the mix of different networked solutions (in-house and outsourced) that the military rely on for running activities, as well as for maintaining communication lines among its three branches. But it serves to highlight the daunting scope of providing security and defense for Brazil in the Digital Era.

Despite the Brazilian growing reliance on ICT, studying its security policy towards cyberspace might be a particularly daunting task. The lack of information on the subject – even in Portuguese – is an obstacle that any researcher will face. Furthermore, the key official documents dealing with the topic, the *National Strategy of Defense* (NSD) and the *White Paper to Guide Future Defense Priorities*, are sometimes dully repetitive and little enlightening. Both documents are, nonetheless, landmarks in defense policymaking in Brazil. They are part of a movement towards transparency and civilian control over the military, which started with the promulgation of the 1988 Constitution and culminated in the creation of a civilian-led Ministry of Defense (MD) in 1999, responsible for all three branches of the armed forces. Those documents also reflect efforts taken in order to staff the MD with its own professional defense bureaucracy[7] while devising the notion that national development is tightly bound to national defense. (Brazil, 2005; 2008b; 2012) Understanding the broader context that helped shaping these provisions is thus necessary in order to assess the Brazilian approach towards cyberspace.

[5] For instance, the Ipê Network – the first Brazilian point of access to the global Internet – operates under the responsibility of the Ministry of Science and Technology and is dedicated to the interconnection of education and research institutions. For further information, please see: http://www.rnp.br/. The Ministry of Planning, Management, and Budgeting is setting up a network called Infovia to supply Brasília (DF), Brazil's capital, with a reliable, exclusive and secure backbone for telephone and Internet communication among agencies of the Federal Government. This model of network is already in place in different states and cities of Brazil. Please see: http://www.governoeletronico.gov.br/acoes-e-projetos/infovia for further information. Recently, Brazil reactivated Telebras. The company, which was the former state-owned monopolistic telephone company running under the responsibility of the Ministry of Communications is the solution adopted by the government to overcome some market distortions in the supply of broadband Internet to some areas of the country. The company was put in charge of building the infrastructure toe advance the National Broadband Plan. It also is supposed to function as an Internet Service Provider. More information about Telebras on: http://www.telebras.com.br/a_telebras.php. For details on the scope of the Brazilian National Broadband plan, see: http://www.mc.gov.br/acoes-e-programas/programa-nacional-de-banda-larga-pnbl. See also the case of the cities of Porto Alegre (RS) and Belo Horizonte (MG), respectively, on http://www.procempa.com.br/default.php?p_secao=19 and http://pwweb2.procempa.com.br/pmpa/prefpoa/abemtic/usu_doc/prodabel.pdf. All websites were last accessed on: 01/21/2013.

[6] For a broader (but still partial) view of the Brazilian cyberspace, please see the technical information provided by ANATEL regarding telecom networks in the country, on: http://www.anatel.gov.br/Portal/exibirPortalInternet.do#. Last accessed: 01/23/2012.

[7] According to Fishman and Manwaring (2011), the MD was initially staffed by "an agglomeration of foreigners," meaning that the Ministry was staffed by technicians and professionals from Petrobras, the Bank of Brazil, and various other government agencies.

The years that followed the 21-year period of military control over Brazil were marked by severe political and economic difficulties. In the political realm, former President Fernando Collor's impeachment and corruption-related scandals distressed the emergent Brazilian democracy, while economic difficulties were mainly related to the necessity to curb inflation, to establish the basis for long-term stability and growth, and to reduce Brazil's extreme socioeconomic inequalities. At the same time, the Brazilian foreign policy adopted a more globalist-oriented view of world politics, which drifted away the realist military influence over the country's international affairs. According to Cervo and Bueno (2002:469), "by separating the two strategic fields [the doctrine of security that guided foreign policy during the military regime and the defense policy], (…) [Brazil] distanced itself from realism and embarked in utopia." In other words, the country's foreign policy underplayed force as a means of action in international relations in favor of persuasion and soft power. It is therefore not astonishing to notice that substantial military reforms have been postponed for almost a decade after liberalization. (Vizentini, 2005)

The first *National Policy of Defense* (NPD) was published in 1996 during former President Fernando Henrique Cardoso's term. The NPD made public the country's security priorities for the first time in history, and thus represented a major milestone for the formulation of a national defense agenda. It was built around two central pillars: active diplomacy (peaceful resolution of conflicts) and conventional deterrence. The document was designed in order to guarantee the country's sovereignty and the safety of national wealth; to guarantee respect for the rule of law and democratic institutions; to maintain the national unity; to protect citizen rights and the Brazilian interests abroad; to provide the country with a more significant role in international affairs; and to contribute to the maintenance of international peace and security. (Brazil, 1996; Oliveira, 2005; Costa, 2006)

The NPD also determined the establishment of an autonomous Ministry of Defense (MD) run by civilian administration to subordinate all three branches of the armed forces (the Air Force, the Navy, and the Army), which happened three years after the document was released, in 1999. The creation of the MD meant an important step towards the consolidation of democracy in the country, as it allowed increased civilian control over the military, a tendency that has been widespread all over Latin America since the late 1980s.[8] Once implemented, the Ministry allowed the development of a more cohesive discourse for the drafting of the second NPD, and represented a breakthrough in terms of institutionalization in the field of defense in Brazil. (Fuccille, 2006; Pagliari, 2009)

The second NPD, released during the first term of President Luiz Inácio Lula da Silva in 2005, expanded the concept of security used so far to incorporate an even broader approach whereby political, economic, environmental and social factors might also be seen as threats to the state. Moreover, the document emphasized the threats posed by non-state actors to both national and international security. Following the former policies stipulations, the new NPD also characterized South America as a peaceful continent, despite recognizing the existence of some zones of instability and the occurrence of transnational organized crime in the region. The need to sustain national sovereignty and the defense of the state were reaffirmed as important means of curbing such issues. The commitment to regional integration was also reiterated, as well as the protection of borders and sensitive areas as the "Green Amazon" (land and river areas within the Amazon Basin) and the "Blue Amazon" (coastal areas where major hydro-carbon and other resources are located). (Brazil, 2005)

All these efforts, however important, did not address cybersecurity issues in depth. Actually, the very first national document to mention anything "cyber-" was the second NPD: "To minimize the harm a cyber attack may cause, it is essential to continuously improve safety devices and to adopt procedures

[8] In fact, Brazil was the last country in the region to unify the military under a single ministry.

to reduce the vulnerability of [computer] systems and allow their prompt recovery." (Brazil, 2005) The subject was left aside from the political debate until 2008, when the *National Strategy of Defense* was released.

THE NATIONAL STRATEGY OF DEFENSE AND THE WHITE PAPER TO GUIDE FUTURE DEFENSE PRIORITIES

In the beginning of his second term as President of Brazil, Lula da Silva directed the development of the *National Strategy of Defense* (NSD). In the months leading up to the release of the document, a Ministerial Committee was established to design it. The Committee was chaired by the former Minister of Defense Nelson Jobim and coordinated by the former Minister-in-Chief of the Secretariat for Strategic Affairs of the Presidency Roberto Mangabeira Unger, and worked in close consultations with civilian and military experts. The document that ensued from the effort focuses on middle and long term strategic objectives for the country, and aims at modernizing the national defense structure acting upon three structuring axes: (i) the reorganization of the armed forces, (ii) the restructuring of Brazilian defense industry, and (iii) the composition of the troops and the future of the Mandatory Military Service. Along with these guidelines, the role of three "decisive sectors for national defense" is discussed: "space", "nuclear", and "cybernetics [sic]."

The NSD thus identifies the need for the development of autonomous technological capabilities in the aforementioned sectors by acknowledging that "whoever does not master critical technologies is neither independent for defense nor for development." (Brazil, 2008b:09) Despite recognizing that "these sectors transcend the border line between development and defense, between the civilian and the military" (Brazil, 2008b:12), the NSD assigns each branch of the armed forces specific mandates to develop each of the decisive sectors.

Special attention is given to the interaction between the "space" and the "cybernetics" [sic] sectors, as the document understands that they, combined, will "enable that the capacity to see one's own country do not depend on foreign technology, and that the armed forces, together, can network supported by a space-based monitoring system." [sic] (Brazil, 2008b:12)

Also according to the NSD,

> "[c]apacity building on cybernetics will be focused on the widest spectrum of industrial, educational and military uses. As a priority, it will include the technologies of communication between all contingents of the armed forces, in order to ensure their capacity to network. They will consider the power of communication between the contingents of the armed forces and space vehicles." (Brazil, 2008b:33)

As to "cybernetics" alone, the NSD simply foresees the establishment of "an organization in charge of developing cybernetic capacities on the industrial and military themes." (Brazil, 2008b:33) Only two years after the release of the NSD, the first steps for the creation of the said organization were taken.

In 2010, the Command of the Army adopted Ordinances ("Portarias") n. 666 and n. 667, which established the Brazilian Cyber Defense Center Nucleus (NU CDCiber) under the responsibility of the Army's Department of Science and Technology. During 2011 and 2012, the Army advanced with the institutionalization of the Center. NU CDCiber's first task was the protection of the network upon which relied the United Nations Conference on Sustainable Development (Rio +20), held in Rio de Janeiro in 2012.[9]

[9] During the II Brazilian Internet Forum, held in Recife in July 2012, Lt. Col. Cláudio Borges Coelho from the Brazilian Army detailed the operation: around R$ 20 million (approximately US$ 10 million) were spent to "ensure the cyber security" of the Conference. The overall mission of the armed forces comprised the protection of lands, waters and the air surrounding the Conference center, as well as counter-terrorism and cybersecurity. The military devised efforts to

In 2012, Brazil adopted the *White Paper to Guide Future Defense Priorities*. Among other provisions, the document foresees the creation of a full-fledged Brazilian Center for Cyberdefense (CDCiber) by 2015. The main distinction between the NU CDCiber and the CDCiber deals with institutionalization: the latter is expected to be formally established through a Presidential Decree aimed at changing the regimental structure of the Army.[10]

The White Paper provides details as to how the armed forces will implement the NSD, which laid ground for more open, transparent communication of the country's defense and security objectives. It resulted from a series of seminars held throughout the country in 2012, broken down by the strategic themes outlined in the Paper. Among the themes comprised by the document stand the strategic scenario for the 21st century; national defense policy and strategy; modernization of the armed forces; rationalization and adaptation of defense structures; economic support of national defense; separate analyses on the Army, Navy and Air Force, and finally peacekeeping operations and humanitarian aid. The three decisive sectors pointed by the NSD are also subject of brief scrutiny.

Regarding "cybernetics," the White Paper stresses that "the protection of cyberspace covers a wide range of areas such as training, intelligence, scientific research, doctrine, preparation and operational employment and personnel management. It also comprises protecting their own assets and the ability to networked operations." (Brazil, 2012:49) In this sense, the text does not go far beyond what was previously stated in the 2008 Plan. On the other hand, it reinforces the call on the military to design forces to meet such requirements, on the defense industry to equip the armed forces accordingly, and on the people to serve a role in the execution of the policy.

But the White Paper's greatest importance actually lies in some short-term actions envisioned for cyber defense, such as building CDCiber's permanent headquarters and the acquisition of support infrastructure, the purchase of equipment and the training of human resources, the procurement of hardware and software solutions for cyber defense, and the implementation of structuring cyber-related projects, which would ultimately increase the country's ability to respond to both national and international threats. (Brazil, 2012:198) All these actions are covered by the so-called Cyber Defense Project, which aims at investing almost R$ 840 million (US$ 420 million) up to 2031. The Project is headed by the Army, but minor efforts are also expected to be launched by the other branches of the armed forces, with an estimated budget of R$ 58 million (US$ 29 million) more.

interoperate with the Federal Police, the Brazilian Agency for Telecommunications (ANATEL), and the Brazilian National Computer Emergency Response Team (CERT.br) of the Brazilian Internet Steering Committee (CGI.br). The expected challenges were said to be, among others, website defacements and the need to reconfigure the network in virtue of overload and tentative attacks. In the occasion, Anonymous managed to post a video on the Conference homepage, protesting against the lack of participation of civil society in the high-level debates on climate change that took place. Also, in a coordinated effort, several activists took down a great number of websites, among them, the Brazilian Senate's website, the website of the Office of the UN in Brazil, and the website of the National Institute for Agrarian Reform and Colonization. A detailed account of the Annonymous action can be seen on the following website: http://www.tecmundo.com.br/ataque-hacker/25395-anonymous-brasil-ophackinrio-tira-do-ar-dezenas-de-sites-governamentais.htm. Last accessed: 11/24/2012.

[10] According to an interview given by Gen. José Carlos dos Santos – the responsible for NU CDCiber – to the largest newspaper in Brazil (*Folha de São Paulo*) in May 2012, the Decree was being analyzed by the Ministry of Planning, Management and Budget before being sent to President Dilma Rousseff's office for her final decision on the matter. Interview available on: http://www1.folha.uol.com.br/tec/1085498-general-detalha-implantacao-do-centro-de-defesa-cibernetica-novo-orgao-brasileiro.shtml. Last accessed: 11/23/2012.

THE GREEN BOOK ON BRAZIL'S CYBERSECURITY AND THE (UPCOMING) NATIONAL CYBERSECURITY POLICY

Efforts on the matter are not only under the responsibility of the Ministry of Defense. The Institutional Security Cabinet of the President's Office has set up a Department of Information and Communications Security (DSIC), responsible for "planning and coordinating the cyber and information and communications security of the Federal government in Brazil." (Brazil, 2010c) Despite having a narrow (the Federal sphere) and developmental (capacity building and risk mitigation) scope, the Department, in partnership with the University of Brasilia, functions as a clearinghouse for cyber-related information. DSIC has been working in close collaboration with other branches of the Brazilian government (including the military) in order to foster the adoption of cybersecurity principles, best practices, and standards for safety and security engineering of information systems. In 2010, the department issued a *Reference Guide for the Security of Critical Information Infrastructures*. (Canongia, Gonçalves Jr., & Mandarino, 2010) The publication describes common threats and vulnerabilities (related to hardware, software, networks, peopleware, etc.), and recommends several policies focused on resilience and redundancy of information systems, as well as on capacity-building schemes aimed at creating "a culture of cyber and information security" within the bureaucracy and the population at large. In the same year, DSIC published the *Green Book on Brazil's Cybersecurity*. (Canongia & Mandarino, 2010) The Green Book highlights the challenges Brazil has to tackle in terms of cybersecurity. They range from economic, social and political-institutional aspects (such as the creation of stimuli for the national IT industry and the adaptation of the legal framework surrounding ICT-enactment in the public sector), to strategic aspects (such as the importance of developing in-house capability and the adoption of open source software). The idea behind the publication is to make the Brazilian population sensitive of the importance of the topic, so that it can fully participate in the open debates that will be entertained for the adoption of the White Paper, or the "National Cybersecurity Policy," in a near time in the future.

***

These efforts show Brazil seems to be following what is possibly the hippest trend in Security Studies: the urgent tackling of what has been commonly called "cyber-"related threats. In fact, this trend has pushed governments throughout South America towards developing similar programs. Efforts have also been made in the multilateral level. Regional organizations like the Southern Common Market (Mercosur) and the Union of South American Nations (Unasur) have established particular *fora* for debating transnational cybercrimes and cyberterrorism.[11]

[11] Within Mercosur, the topic is discussed together with other actions aimed at curbing organized crime, cross-border trafficking, etc. On the other hand, Unasur has implemented a special Working Group to establish regional policies and mechanisms to address cyber threats and information technology in terms of defense. On the hemispheric level, it is relevant to recall that the Organization for American States (OAS) adopted, in 2004, a "A Comprehensive Inter-American Cybersecurity Strategy" with the objective of developing "a culture of cybersecurity in the Americas by taking effective preventive measures to anticipate, address, and respond to cyberattacks, whatever their origin, fighting against cyber threats and cybercrime, criminalizing attacks against cyberspace, protecting critical infrastructure and securing networked systems." The strategy has a civilian character and aims at fostering the development of legal tools for the combat of all sorts of cyber crime. It set up an "Inter-American Alert, Watch, and Warning Network" in order to "rapidly disseminate cybersecurity information and respond to crises, incidents, and threats to computer security." Despite having a larger scope than the scope of this study, this initiative is worth quoting, for it contends without further qualification and precision that "criminals such as 'hackers,' organized crime groups, and terrorists are increasingly exploiting the Internet for illicit purposes and engineering new methods of using the Internet to commit and facilitate crime. These illegal activities, commonly referred to as 'cyber-crimes,' hinder the growth and development of the Internet by fostering the fear that the Internet is neither a secure nor a trustworthy medium for conducting personal, government, or business transactions." This wording is addressed under section 4 of this paper.

While these moves demonstrate South American governments are completely aware of one of the most important current security threats, they must be interpreted with caution: these countries might be replicating controversies that still are not fully comprehended by part of the international community.

CONCLUSIONS

As seen hitherto, Brazil has been pursuing information and communications security, as well as cybersecurity and defense through the integrated efforts of the leading DSIC (attached to the office of the President) and through Army's NU CDCiber (in the future, just CDCiber). The fog of (cyber)war blurs the boundaries between those roles. Bellow, we turn to the evaluation of the approach adopted by Brazil in 2008/2012 to deal with the complex array of "cyber issues" in light of the content presented in section 3. Highlighting the positive and negative aspects of such an enterprise is a small first step that can contribute to qualify research and public policymaking.

Positive Aspects

Among the positive aspects of the Brazilian endeavor, the first one to be highlighted is the country's willingness to cope with the challenges inherent to the digitalization of society at large. The incorporation of topics such as information and communications security, and cyberdefense in the policy agenda of the country seems to be a proper initial response for the increasing reliance on cyberspace of a myriad of productive activities in different areas of society. It also underlines that Brazil is tuned to what is happening all over the world, both in terms of disruptive events and policy trends. Before the attacks to web sites that happened during Rio +20 Brazil had not registered any major cyber incident.[12] Even before 2012 the MD and the Institutional Security Cabinet of the President's Office had already been taking measures aimed at mitigating ICT-related risks and at forestalling threats to information systems in general.

That two-front action reveals another positive aspect identified by our evaluation: the Brazilian initiative counts on both civilian and military facets. The first is responsible for the formulation of principles and norms, as well as best practices and frameworks, all intended to foster safety and security engineering in the development and adoption of IT solutions in the federal government. The latter has a more restrict and pragmatic – despite more complex - mandate: the development of defensive and offensive capabilities related to cyberspace as power leverage for Brazil's conducting its international affairs. This specialized approach, if integrated and coordinated, can increase the resilience of the country in face of cyber threats, for it has the potential of creating a common approach for the organization and governance of Brazil's cyberspace, which can facilitate the planning and orchestration of emergency responses and of defense policy-making and operations. Evidence of this trend can be found in the express recognition by MD officials that a collaborative approach to cyber security and defense could yield better results in terms of preparation for dealing with and of the appropriateness and effectiveness of responses to cyber events. Another piece of evidence of this trend

[12] In 2009, Brazil suffered severe blackouts as a result of a general failure of transmission lines related to the Itaipu hydroelectric plant, owned by Brazil and Paraguay. Ninety per cent of the territory of the latter was affected and remained in the dark for more than half an hour. Four different states in Brazil were also severely affected, and around ninety million people lost electric power for more than five hours. Some days before the blackouts, CBS's "60 Minutes" program had displayed a piece of news contending that prior blackouts that happened in Brazil (2005 and 2007), as well as in the U.S., were caused by hack attacks. The Brazilian government promptly denied those claims, explaining that dirty insulators on transmission towers caused the blackouts. Some leaked diplomatic cables released by Wikileaks in 2010 reinforced the government's explanation. For further information on the topic, see: http://www.wired.com/threatlevel/2010/12/brazil-blackout/. Last accessed: 01/20/2013.

can be found in the assembly of a joint task force responsible for assuring the security and defense of the networks that supported communication channels during Rio +20. A closer scrutiny of the action of that task force reveals that several of the IT-systems adopted for the conference were not off-the-shelf. They were customized not only in order to better suit the needs of the users, but also as a way of increasing their inviolability.

When it comes to the issue of offensive capabilities, though, the boundaries of what is legal and what is not within the scope of International Law are completely blurred. This lack of common ground on the international level coupled with the concerns raised before in this text – about the complexity of offense on cyberspace – reveals a potential pitfall for the Brazilian strategy: developing offensive capabilities that deal essentially with the surveillance of other actors in the context of a normative vacuum can lead the country to cross the line of legality and to decrease instead of increasing its national security.

A final aspect that must be highlighted is the collaborative and participatory policy-making process that characterizes the adoption of documents such as the END, the White Paper, and the Green Book presented in section 2. During the preparatory phase, as well as in the review and publication phases, the MD and the Department of Information and Communications Security of the President's Cabinet have realized public seminars and openly published documents on the Web to allow the participation of citizens and stakeholders interested in the debates. For instance, in the case of the *White Paper to Guide Future Defense Priorities*, the MD conducted a series of six national seminars in the five major regions of Brazil to present and debate the document through the lenses of specialists, and to gather inputs from the participants. In the case of the *Green Book on Brazil's Cybersecurity*, DSIC started publicizing the document with the intention of fostering the dialogue among different state and non-state actors that shall serve as the basis for the production of a more definite White Book on the matter. These efforts reflect the willingness of the Brazilian state not only to broaden dialogue between civil society, the public administration, and the military, but also to strengthen the country's transparency and democracy levels.

Negative Aspects

Despite having adopted some very sound paths for enhancing its security and increasing its defense capabilities in the Digital Era, some characteristics of the Brazilian approach are not entirely satisfactory, and might have some severe side effects not only in terms of national security, but also in terms of broader societal relations.

The first questionable point is the fact that Brazil treats "cybernetics" as a fifth domain for waging war. As pointed out above, two lines of reasoning contradict this position. Firstly, the progressive digital convergence of all media to Internet-based technologies, as well as the pervasive character of the Net, tends to "cyber" everything. But this homogeneous set of systems, however big, is still only part of cyberspace. As long as the level of interconnectivity among IT systems matters, it is practically impossible to determine the full scope of cyberspace. Secondly, granting a system more or less interconnectivity is a decision taken mainly by the people who design and develop such systems. And engineering decisions cannot be segregated from broader sociopolitical contexts. Thus, it might be relevant to retrieve "cyber-"s original meaning from its Greek root. Instead of narrowly focusing only on technological systems, a turn to the myriad of institutional and organizational settings that influence the adoption of those systems could be more fruitful for the development of security and defense policies. Addressing, for instance, the *locus* of ICT-related decisions within the military and its ties

with other civilian agencies may be better than just institutionalizing cyber cabinets in charge of developing policies to be applied elsewhere.

From this perspective arise the following questions: what is the precise role of cyber commands and cyber battalions? How should they relate to the overarching organization of government? Should they be a privileged group of experts capable of operating IT systems more or less connected to each other even if agreed that cyberspace has no clearly defined boundaries? Or should they function as focal points for the adaptation of all other sectors of the military to better operate in the Digital Era? Shouldn't cyber capabilities and skills be a fundamental competence for top-ranking officials in charge of developing military strategies in the 21st century?

Moreover, governance transcends the sphere of government, for it also encompasses the whole of state–society relations. As shown in section 3, the securitization of cyberspace has been based on a very diffuse perception of what the contemporary threats to national and international security are. State and non-state actors have been equated as major foes. This is also the case in Brazil. Take, for instance, the list of cyberspace-related threats presented by public officials during the seminars that preceded the White Paper's release: in order of increasing severity, hacktivism, cybercrimes, espionage, sabotage, terrorism and war were commonly mentioned. It is pretty rare, though, to see such list enriched with a thorough evaluation of the inherent complexity of each of those acts.

Treating those categories alike tend to disregard important power asymmetries that are analytically and practically relevant to compare and contrast states among themselves, and states *vis-à-vis* non-state actors. While the Internet offers a cheap and easy way of entering cyberspace, it does not automatically mean that they are synonyms. Since cyberspace is a complex set of more or less interconnected information systems, the capacity to mobilize resources (political, financial, societal, human, technical, etc.) to explore – and eventually exploit – them matters as it does in every other realm of social life. An intelligence report on China's cyber activities recently published by the private information security company Mandiant shows that the country "maintains an extensive infrastructure of computer systems around the world", which "implies a large organization with at least dozens, but potentially hundreds of human operators." (Mandiant, 2013:04-05) In the U.S., for instance, amidst several budgetary constraints to the military, investment on cyber security and defense has steadily risen. In the near future, it is hard to believe that non-state actors might match state capacity, and that states with less overall capacity might overcome asymmetries by merely turning to the "cyber".

The equation of cyber foes has two major consequences. In the first place, it makes it more difficult to adopt appropriate policies for dealing with cyber insecurity. As a result, it can compromise the adoption of preemptive measures and actual responses to disruptive cyber events. After all, the requirements for dealing with web page defacements are different than those required for protecting and assuring air-gapped communication lines. But more importantly, the fog that surrounds the precise definition of cyber threats and foes has a lot to do with the proper balance between the fundamental rights of individuals (civil and political) and the rights of the states (that enable them to fulfill their role in the provision of security, justice and welfare). What are the limits for state action in relation to the privacy of its citizens? In virtue of the decentralized and distributed architecture of cyberspace, what sort of extraterritorial side effects should one expect from the monitoring and surveillance activities developed by a state in order either to secure or to defend its own cyberspace or to explore other actors' cyberspace? Are the penalties that have been summoned to cyber events reasonable and suitable for what they entail? How open and participatory are decision-making processes that deal with such trade-off?

The Brazilian case shows that it is reasonable to say that despite the participatory approach to the development of its initial steps for dealing with cyber security and defense, there is a great lack of

oversight and accountability of the implementation and institutionalization processes detailed by the documents reviewed in section 2. Budgetary information is neither complete nor detailed. One cannot find a proper justification for the timetable adopted for the different projects and subprojects that congregate the defense priorities established by the country. Technical options are outside public scrutiny, for they deal with sensitive information. It does not mean, however, that the general public cannot be part of the decisions that form cyber security in Brazil. Involving the citizenry in the decision-making processes that determine the contours of a general strategy to secure cyberspace can increase its legitimacy, as well as make its implementation more easily accountable.

Despite being part of the Brazilian strategies, it is extremely difficult to determine based on the evidence so far existent whether the collaborative and participatory approach is a permanent feature of the Brazilian endeavor. Institutional and organizational aspects of the Brazilian federal government (such as inter-bureaucratic competition, the periodic governmental electoral transition, political and technical disagreement on policy lines to be pursued in the military and in the civilian sector, etc.) might contribute to the derailment of the initial coordinated and collaborative approach.

As it is impossible to definitely address all of those concerns, a follow-up of the future developments in the case of Brazil can enlighten several of the doubts raised in this text. Also, those positive and negative aspects do not seem to be an exclusive feature of the Brazilian case, a fact that pave the way for further inquiry in the field.

REFERENCES

Brazil (1996). Política de Defesa Nacional. Available on: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm. Last accessed: 02/20/2013.

Brazil (2005). Política de Defesa Nacional. Available on: http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm. Last accessed: 02/20/2013.

Brazil (2008a). Estratégia Nacional de Defesa. Available on: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Decreto/D6703.htm. Last accessed: 02/20/2013.

Brazil (2008b). National Strategy of Defense. Available on: http://www.defesa.gov.br/projetosweb/estrategia/arquivos/estrategia_defesa_nacional_ingles.pdf. Last accessed: 02/20/2013.

Brazil (2010) Census 2010. Available on: http://censo2010.ibge.gov.br/. Last accessed: 02/20/2013.

Brazil (2010a). Ordinance n. 666, issued by the Command of the Army on August 4th, 2010. Available on: http://tinyurl.com/aebz5yw. Last accessed: 02/19/2013.

Brazil (2010b). Ordinance n. 667, issued by the Command of the Army on August 4th, 2010. Available on: http://tinyurl.com/aebz5yw. Last accessed: 02/19/2013.

Brazil (2010c). Presidential Decree n. 7.411/2010, issued on December 12th, 2010. Available on: http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2010/Decreto/D7411.htm. Last accessed: 02/20/2013.

Brazil (2012). Livro Branco de Defesa Nacional. Available on: https://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf. Last accessed: 02/21/2013.

Canabarro, D. and T. Borne (2013). Reflections on the Fog of (Cyber)War. NCDG Policy Working Paper No. XX-2013. Available on: http://www.umass.edu/digitalcenter/research/working_papers/13_001_Canabarro-Borne_FogofCyberWar.pdf. Last accessed: 03/15/2013.

Cervo A. L. and C. Bueno (2002). História da Política Exterior do Brasil. Brasília, DF, Brazil: Editora UnB.

CETIC.br (2011). ICT Households and Enterprises (2011) - Survey on the Use of InformatIon and CommunIcation Technologies in Brazil. Available on: http://cetic.br. Last accessed: 01/25/2013.

Costa, T. G. (2006). "Em Busca da Relevância: Os Desafios do Brasil na Segurança Internacional do Pós-Guerra Fria." Relações Internacionais do Brasil: Temas e Agendas. H. OLIVEIRA and A. C. LESSA. São Paulo, SP, Brasil: Saraiva.

Drake, W. (2008). “Introduction. Governing Global Electronic Networks: International Perspective on Policy and Power.” W. J. DRAKE and E. J. WILSON. London, UK, MIT Press.

Fishman A. and M. Manwaring (2011). “Brazil’s Security Strategy and Defense Doctrine.” Colloquium Brief. U.S. Army War College, Strategic Studies Institute.

Fuccille, A. Democracia e Questão Militar: A Criação do Ministério da Defesa no Brasil. PhD Dissertation (Political Science). Instituto de Filosofia e Ciências Humanas, Programa de Pós-Graduação em Ciência Política, Universidade Estadual de Campinas (UNICAMP), Campinas, SP, Brazil. Available on: http://cutter.unicamp.br/document/?code=vtls000378085. Last accessed: 09/10/2012.

ITU (2011). World Telecommunication/ICT Indicators Database. Available on: http://www.itu.int/ITU-D/ict/statistics/. Last accessed: 12/05/2012.

Mandiant (2013). APT1: Exposing One of China's Cyber Espionage Units. Available on: http://intelreport.mandiant.com/. Last accessed: 02/21/2013.

Miranda, P., H. Kume, et al. (2011). Liberalização do Comércio de Serviços: O Caso do Setor de Telecomunicações no Brasil. Rio de Janeiro, RJ, Brasil: IPEA.

OAS (2004). A Comprehensive Inter-American Cybersecurity Strategy: A Multidimensional and Multidisciplinary Approach to Creating a Culture of Cybersecurity. Available on: http://www.oas.org/juridico/english/cyber_security.htm. Last accessed: 12/28/2012.

Oliveira, H. A. (2005). Política Externa Brasileira. São Paulo, SP, Brasil: Saraiva.

Pagliari, G. C. (2009). O Brasil e a Segurança na América do Sul. São Paulo, SP, Brasil: Juruá Editora.

Schiller, D. (2000). Digital Capitalism: Networking the Global Market System. Cambridge, MA, USA: MIT Press.

Vizentini, P. G. F. (2005). “De FHC a Lula: Uma Década de Política Externa (1995-2005).” Civitas – Revista de Ciências Sociais, 5:2, 381-397.