DECONSTRUCTING CYBER SECURITY IN BRAZIL:

Threats and Responses

Gustavo Diniz, Robert Muggah and Misha Glenny

Abstract

Brazil is doubling down on its cyber-security architecture while simultaneously consolidating its emerging power status. Although organized crime is one of the major threats to Brazilian cyberspace, resources are focused instead on military solutions better suited to the exceptional case of warfare. There is less emphasis on expanding law enforcement capabilities to identify and respond to cyber-crime and related digital malfeasance. Due to the absence of a unified government position on the issue or reliable data, Brazil has evolved an imbalanced approach to cyber-security. If Brazil is to rebalance its approach, it needs to fill knowledge gaps. At a minimum, policy makers require a better understanding of the strategies, tactics and resources of hackers and cyber-crime groups, the ways in which traditional crime is migrating online and the implications of new surveillance technologies. The government should also encourage a broad debate with a clear communications strategy about the requirements of cyber-security and what forms this might take. More critical reflection on the form and content of measured and efficient strategies to engage cyber threats is also needed. Improved coordination between state police forces to better anticipate and respond to cyber-crime is essential. If Brazil is to build a robust and effective cyber-security strategy, an informed debate must begin immediately.

CONTENTS

DECONSTRUCTING CYBER SECURITY IN BRAZIL: Threats and Responses*

Gustavo Diniz, Robert Muggah and Misha Glenny [1]

Introduction

Brazil is confronted with a wide variety of so-called *cyber threats*, including online scams, cybercrime, and digital surveillance. Not all of these threats are necessarily equal. Arguably the most serious and widespread risk is economically-motivated cybercrime – the targeting of private banks, firms and individual consumers for profit. Another important set of cyber threats is emerging from domestic and foreign hacktivist groups seeking to disrupt government services, websites and also corporate targets. The massive popular protests of June-August 2013, for example, coincided with an uptick in hacktivist activism. Finally, the revelations by Edward Snowden that Brazil's official communication networks were routinely spied on by the US National Security Agency (NSA) gave rise to the specter of a new cyber threat to the country: cyber-espionage and, some fear, cyber-warfare.

And while concerns about cyber threats are growing across Brazil and Latin America, comparatively little is actually known about them. There is virtually no debate about the actors generating the threats, the actors' interests and motivations, how they operate or how they are connected to more traditional criminal or political organizations. Few specialists are undertaking detailed assessments of these various – and in some cases very distinct – cyber threats, much less evaluating public and private sector responses. In spite of a profound lack of knowledge, the Brazilian government has nevertheless rapidly mounted a sprawling cybersecurity and defense infrastructure. Oddly, the response is narrowly focused on just a few dimensions of these threats – especially foreign ones. Of the many institutions involved, the Brazilian Army's *Center for Cyber-defense* (CDCiber) is a core component of the country's defense posture.

Brazil's fast evolving cyber-security apparatus is, to a certain extent, misaligned with actual and emerging threats in cyberspace. Instead of focusing on international and domestic cyber-criminality more narrowly, the state is constructing a response to improve cyber war fighting and anti-terrorism capabilities. This is not to say that there are not clear and present dangers associated with cyber terrorism and cyber warfare. Rather, this *Strategic Paper* finds that the Brazilian government is adopting a securitized approach to cyber threats rather than addressing the most pressing challenges confronting citizens, especially cybercrime. Put succinctly, the state (the agent) is securitizing cyberspace (the referent) on behalf of the people (the audience). When a subject is securitized it is possible to legitimize extraordinary means to solve a perceived problem, including

* The authors would like to thank all those who contributed to this paper. Special thanks to Bernardo Wahl, Marcos Flávio, Delegado Carlos Eduardo Miguel Sobral and URCC-DPF team, Daniel Opperman, Ronaldo Lemos, Walter Capanema, Antoine Nouvet and Rafal Rohozinski.

[1] Gustavo Diniz was a research associate at the Igarapé Institute. Robert Muggah is the research director of the Igarapé Institute, directs research at the SecDev Foundation and is chief social scientist of the SecDev Group. Misha Glenny is an international author on subjects ranging from the Balkans and Brazil to organized crime and cybercrime.

emergency legislation, mobilizing the military or otherwise.[2] This not only has consequences for public policy and spending; the oversized military response also risks compromising citizens' fundamental rights owing to, among other things, pervasive surveillance and censorship. For instance, CDCiber and Brazil's central intelligence agency (ABIN) created social media monitoring platforms in the aftermath of the 2013 protests.

The securitized approach to addressing cyber insecurity in Brazil is consistent with a broader effort to redefine the role of the Brazilian armed forces for the twenty-first century. As Brazil consolidates its democracy, stability and economy, the armed forces are redefining their role and posture in relation non-traditional threats. On the one hand, they are strengthening border control and anti-drug activities.[3] On the other, the armed forces are seeking to expand their reach and influence in the dynamic and constantly evolving domain of cyberspace. Meanwhile, other important public institutions to address cyber threats, such as the Federal Police, are less amply resourced and organized. The development of a militarized cyber-response capacity is thus partly inspired by Brazil´s effort and desire to enhance its geopolitical reach and relevance. As a rising power, Brazil's government is making use not only of the country's nascent cyber-security architecture, but also of its cyber-governance expertise more broadly, to project soft power in bilateral relations and multilateral forums.

This *Strategic Paper* considers the evolution and implications of this securitized turn in the management of Brazil´s cyber commons. The first section provides a panorama of Brazil's cyber-landscape. Section two assesses real and implied threats to Brazil in cyberspace, highlighting national priorities but also lapses in the state´s response. The third section focuses on legal and programmatic responses to these threats, with a particular attention to the role of security institutions. Section four discusses the dilemmas that arise from a heavily militarized approach to cyber-security. It also details how Brazil's efforts to assert itself internationally are shaping the domestic decision-making process in relation to cyber security and defense. The conclusion offers a summary of findings and a set of recommendations to address the challenges of cyber-governance and security in Brazil.

2 See the work of Waever (1995) on securitization.

3 See Diniz and Muggah (2012).

Defining Brazilian cyberspace

Brazil is undergoing a digital revolution with few parallels in the developing world. The rate of digital penetration and social media adoption has risen exponentially over the past decade. During this period, Brazil witnessed a tenfold increase in Internet access and mobile phone subscriptions, with more than half of its population of 200 million people currently online.[4] A number of factors relating to Brazil´s improvements in social and economic development are driving these trends. A relatively stable macroeconomic climate and strongly redistributive social policies resulted in the expansion of the country's middle class. An influx of new consumers simultaneously ratcheted-up the demand for information and communication technologies (ICTs) and transformed the scale of supply at levels commensurate with Brazil's gigantic domestic market.

The emergence of an enlarged and highly connected middle class is shaping Brazil's cyber environment. Improved access to new information technologies has given rise to a wide array of social, political and economic forms of empowerment in Brazil. Not surprisingly, digital empowerment is also accompanied by additional challenges, ranging from mass protest to organized crime. As a middle-income country, Brazil has to fully address its deeply rooted inequalities both online and off. Contradictions are emerging as its public policy makers seek to more fully integrate newly empowered citizens into the country´s democracy and formal economy. And as an emerging power, Brazil also faces dilemmas arising from its increased engagement in global politics. Domestic and international factors therefore play a critical role in shaping Brazilian cyber-governance.

Few other countries have been as dramatically affected by digital empowerment as Brazil. The scale and dynamism of Brazilian cyberspace has reached new heights in recent years. It ranges from the digitally-enhanced mass demonstrations that hit Brazilian streets between June and August of 2013 to the country's routine presence at the top of rankings associated with cybercrime.[5] Brazil is widely recognized as both a perpetrator and a victim of online criminality. What is more, Brazil is still reeling from revelations of espionage conducted by several countries – notably the United States, Canada and the United Kingdom – and has initiated reform processes in the United Nations and domestically. The complex nature of the "cyber threat" – and the way it is interpreted in Brazil [6] – has played a significant role in shaping the country´s cyber-governance and cyber-security architecture.[7]

---

[4] See Internet World Stats website (http://www.Internetworldstats.com), as of December 2013.

[5] The International Telecommunications Union (ITU) defines cybercrime as activities in which computers or networks are employed as tools, targets or places for the achievement of criminal ends. It establishes five categories: 1) offences against the confidentiality, integrity and availability of computer data and systems; 2) content-related offences; 3) computer-related offences; 4) copyright- and trademark-related offences; and 5) complex or combined offenses (like cyber money laundering, cyber-terrorism and warfare, espionage and, to some extent, hacktivism). See ITU (2009).

[6] Our choice for the term "cyber threat" instead of "cybercrime" implies a more expansive view of the real extent of harmful digital activities. Many countries in the developing world, including in Latin America, are exposed to certain "cyber threats" that do not readily fit ITU's strict definition. Moreover, the expression cyber threat accounts for perceptions that also may not necessarily reflect real objective risk. It is important to assess what a society perceives as its primary digital threats and how these are addressed over time.

[7] According to Brazilian practitioners, cyber-security includes "preemptive and repressive actions, normally implying a persistent state of attention and preparedness of the systems and people involved. It is also used to refer to private practices of protection of cyberspace, by individuals and companies". Cyber-defense, by contrast, includes "operational actions deployed for offensive and counter-offensive combats in cyberspace, being commonly linked to countries' military and intelligence services". See Canongia and Mandarino (2009). We also refer to cyber-governance given its linkages with cyber security.

A balanced assessment is required when considering cyber threats and cyber-security responses. It is important to reflect on the powerful interests and symbolic struggles shaping the narrative on what constitutes a digital threat in a given society. A careful parsing of the narrative, and the underlying factors giving rise to it, can highlight how priorities are determined and resources allocated. One can move beyond short-termism to a broader long-term perspective on what shapes the decisions of key actors. It is only by adopting a unvarnished perspective that one can fully understand how cyber-security is conceived, constructed and applied. And these choices matter since they fundamentally influence questions of public security and individual rights to privacy both online and off.

The rise of new technologies

The demographics of Internet usage in Brazil are analogous to a number of other large middle-income countries, though with some significant differences owing to the sheer dimensions of the nation. Specifically, Brazil is well positioned when compared to other powerful emerging economies, particularly within the Brazil, Russia, India, China and South Africa (BRICS) group. Brazil is situated between Russia and China in terms of the percentage of Internet users (of the country's total population).[8] When compared to its neighbors and other emerging powers, however, Brazil is leads the group. Brazil is far ahead of its Latin American and Caribbean (LAC) counterparts in terms of ICTs usage. It has the largest on- and offline populations in Latin America: there are approximately 110 million Internet users in the country, or around 54.2 per cent of the population.[9] This represents nearly double the number of total users of the second most digitally-connected country in Latin America, Mexico.[10]

Several characteristics associated with Brazilian Internet usage warrant special attention. For one, Brazilians are avid producers and users of social media.[11] If the LAC region is the world's largest consumer of social media, this is largely due to Brazil's voracious appetite for online networking. Brazilians spend on average 2.2 hours per week on social media platforms such as Facebook.[12] Almost 60 per cent of Internet users in Brazil are registered on Facebook, second only to the United States in number of profiles.[13] The same is true when it comes to Twitter: Brazilians own 33 million accounts and registrations continue upwards.[14] Brazilians tend to both drive and follow trending topics; 20.5 per cent of the country's Internet users visit the platform regularly. Globally, Brazil is fifth in overall in Twitter use.[15]

---

[8] Russia has 87 million internet users (61.4%), India 195 million (15.2%), China 621 million (45.8%), and South Africa 24 million (49%). See Internet World Stats website (2013).

[9] See Internet World Stats website, as of December 2013.

[10] Mexico has 52 million internet users or 43.5% of penetration. See Internet World Stats website (2013).

[11] Latin Americans spent 56% more time on social networking platforms than the global average. See http://thenextweb.com/twitter/2013/01/16/twitter-to-open-office-in-brazil-its-second-biggest-market-after-the-us-in-accounts/.

[12] See http://online.wsj.com/news/articles/SB10001424127887323301104578257950857891898.

[13] See Internet World Stats websites (results as of December 2013).

[14] See http://semiocast.com/en/publications/2012_01_31_Brazil_becomes_2nd_country_on_Twitter_superseds_Japan.

[15] See http://www.billhartzer.com/pages/comscore-twitter-latin-america-usage/.

Second, in recent years Brazil has witnessed a massive surge of electronic, economic and financial activities moving online. Brazil boasts high levels of engagement with online financial services, similar to upper-income settings in North America and Western Europe. The digital economy is evolving lockstep with the Brazilian economy as a whole. When it comes to e-commerce, the total value of transactions in 2012 was US$ 11.3 billion, representing an annual increase of 25 per cent in comparison with 2011.[16] But it is in the e-banking sector that Brazil shows the real strength of its digital economy. Almost all Brazilian accounts are today accessed via the Internet. Overall, the banking customer base grew 8 per cent in 2012 to include 54 million people, representing 42 million internet banking accounts and 3.4 million mobile accounts, an 11 per cent and 49 per cent increase, respectively, in relation to 2011.[17] These are unusually large numbers and illustrate a distinct characteristic of Brazil's cyberspace. Brazil´s cyber-criminals have, predictably, also organized their targets and practices around e-banking systems and users.

A third characteristic of Brazilian Internet usage relates to mobile phone access and usage, which has risen dramatically in the last three years. There is now an average of more than two subscriptions per person.[18] The vast majority of mobile phones still used for personal calls or sending text messages. However, a strong shift towards smartphones and tablets is now underway. In the first half of 2012, the number of smart phones doubled, reaching 60.1 million devices.[19] Mobile phones with broadband Internet connection already make up around 36 per cent of the cellphone market in Brazil.[20] The popularity of smartphones is likely to accelerate in the near future. Brazilian authorities are investing heavily in the spread of broadband connections and the transition from 3G networks to 4G networks. These shifts are also partly explained by recent and future mega-sporting events, including the FIFA World Cup (2014) and the Olympics (2016), which are raising demand for faster and more reliable connectivity. The government decided to exempt local smartphone manufacturers from corporate taxes to ensure a reduction in retail prices.[21] Increased access to smartphones (and lower prices) has also been aided by the flooding of the Brazilian market with cheaper Chinese products. [22]

Fourth, there has been a dramatic change in who and how people access the Internet. More than 66 per cent of Brazilian Internet users access the web on a daily basis, while 25 per cent do this at least once a week. While younger people (ages 16 to 34) make up the majority of Internet users, there is no significant difference in terms of hours spent on the net across age groups. Nor are there any significant gender-related differences, at least in terms of usage: there are as many females as males on the web spending more or less the same amount of time.[23] Public policies promoting digital inclusion, higher earnings and more inexpensive products are also changing how Brazilians access the net. In 2011, the Internet was accessed 59 per cent of the time from home, 14 per cent from cyber-cafes (Local Area Networks), 12 per cent from work, 8 per cent from someone else's house, 3 per cent from school, 2 per cent from mobile devices and 1 per cent from free public wi-fi areas.[24] Recent studies conducted by CTS-FGV reveal a steep decline in the number of cyber-cafes

16 See http://wyse.com.br/portugues/2012/03/o-comercio-eletronico-no-brasil/.
17 See http://www1.folha.uol.com.br/fsp/mercado/69329-bancos-perdem-r-15-bi-com-fraudes.shtml.
18 See ITU ICTs Data and Statistics at http://www.itu.int/ITU-D/ict/statistics/explorer/index.html.
19 See http://tecnologia.ig.com.br/2013-01-18/entre-os-celulares-usados-no-brasil-36-sao-smartphones-diz-nielsen.html.
20 Ibid.
21 See http://www.redebrasilatual.com.br/tecnologia/2013/04/programa-de-inclusao-digital-deve-reduzir-preco-de-smartphones-nacionais.
22 CTS-FGV presentation during the event Open Development (IDRC – Montevideo, Uruguay, April 2013).
23 See http://www.cetic.br/usuarios/tic/2011-total-brasil/rel-int-03.htm Percentage using internet on a daily basis regarding age: 10-15 (57%); 16-24 (66%); 25-34 (70%); 35-44 (68%); 45-59 (68%); and 60-higher (68%).
24 See http://www.cetic.br/usuarios/tic/2011-total-brasil/rel-int-04a.htm.

over the past few years as the costs of laptops, tablets and phones declines, including in poorer and densely populated areas such as favelas.[25] Even households from the most modest social sectors can now afford new technologies for personal use, so access from home and on mobile devices is fast becoming the rule.

Finally, the extent of Brazilian activity in cyberspace nevertheless still reflects the country's structural inequalities. Differences in income, education and geographic region influence how and whether people access the Internet. For instance, 50 per cent of households in the states of Sao Paulo, Rio de Janeiro, Minas Gerais and Espirito Santo have Internet access, but the percentage plummets to 22 per cent in the Northern region.[26] Furthermore, on average the wealthier classes spend much more time on the Internet than the poor. The proportion of those who go online at least once a week is about 80 per cent for upper-class users, 65 per cent for middle classes, and less than 50 per cent for lower classes. The difference is also clear when it comes to level of education. While 55 per cent of the country's illiterate population goes online on a weekly basis, the amount of time spent on the Internet rises significantly for people with shigher education, such as a college or university degree: 87 per cent go online at least once per week. [27]

Increased connectivity and digital empowerment in Brazil is inextricably related to the country's structural inequalities.[28] This becomes clearer when one analyzes the entire spectrum of users and related activities in Brazil. Organized and disorganized groups are beginning to take advantage of cyberspace, whether to press for political and social change or to advance their own private economic interests, including criminal ones. There are encouraging examples of social movements harnessing the power of new networks and communications infrastructure to push for positive and progressive political transformation. Due in large part to Brazil's formidable structural challenges, there is a growing trend toward exploiting the Internet for personal and criminal gain.

Assessing cyber threats

A wide spectrum treatment of cyber threats is critical in order to begin to overcome misconceptions and address misguided policies. Due to the novelty and technical nature of the issue, governments and citizens are relatively poorly informed about how to respond. Citizens, businesses and institutions often feel that understanding the issues is beyond their capacity or that threats are not relevant to them. Ignorance or misperceptions often result in a failure to address cyber-security threats directly. Strategies, if they are adopted at all, tend to be cobbled together on the basis of spurious and untested premises. There is seldom robust data to drive decision-making. A more evidence-based approach is urgently needed in order to assess cyber threats – one informed by knowledge of the numerous and interconnected risks online. Unfortunately, already scarce time and resources are frequently allocated to less important areas rather than actual primary threats.

---

25 See http://direitorio.fgv.br/node/2507.

26 See www.cetic.br/usuarios/tic/2011-total-brasil/index.htm.

27 54% of people with an elementary education go online at least once per week; this increases to 63% for people with a high school education. See http://www.cetic.br/usuarios/tic/2011-total-brasil/rel-int-03.htm.

28 Digital inclusion indicators in Brazil also show disparities, when compared nationally and internationally. See FGV-CPS (2012a and 2012b) and http://tecnologia.terra.com.br/internet/inclusao-digital-no-brasil-esta-acima-da-media-mundial,c91cfe32cdbda310VgnCLD200000bbcceb0aRCRD.html.

The following section considers conventional cybercrime, complex cyber offenses and emerging threats to help shape the formation of a more sophisticated agenda in Brazil.

Table 1. The three main sets of cyber threats in Brazil

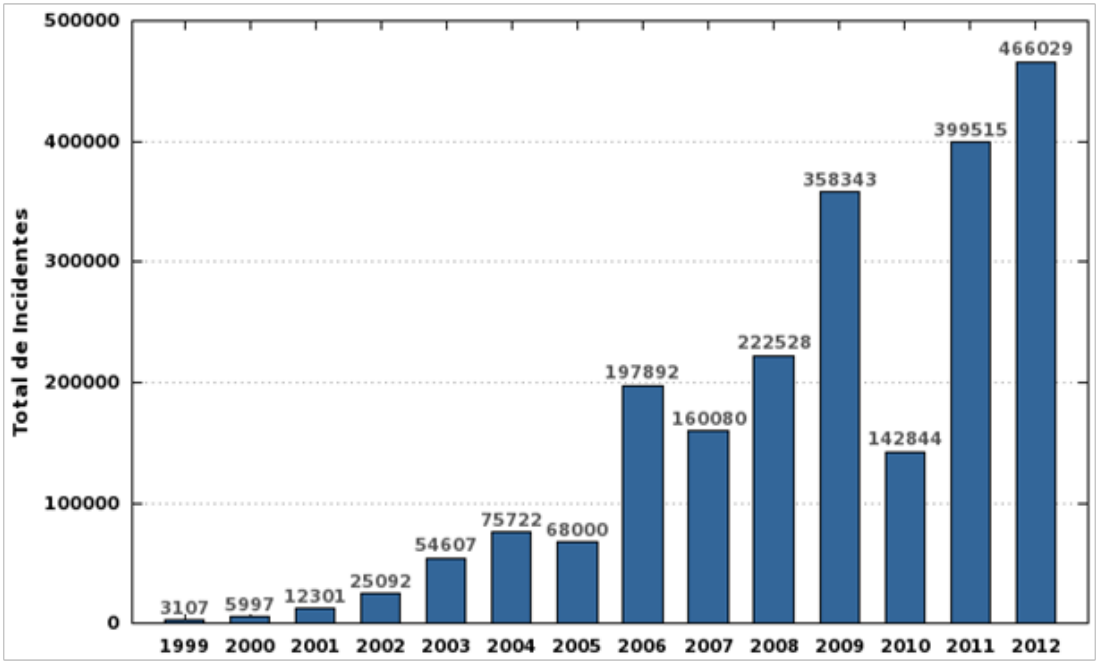
Category	Definition	Examples	Usual government responses	Brazilian reality
Conventional cybercrime	These are the most widespread forms of cyber-offenses in the world and follow the typology proposed by the ITU (2009) [see footnote 5].	Illegal access (cracking), data interception, child pornography, spam, hate speech, banking fraud, identity theft, copyright infringements	Exclusively law enforcement, since it normally embraces traditional crimes that are already categorized in criminal codes	There are two major subsets of conventional cybercrime: 1) economically-motivated (especially banking fraud) and 2) content-related (e.g. racism and child pornography in social media networks)
Complex cybercrime	This considers and expands ITU definition of complex or combined cyber offenses, those that may fall within more than one category of conventional cybercrime.	Cyber-terrorism, cyber-warfare, attacks against critical infrastructure, cyber-espionage, and hacktivism	A mix of intelligence, military and law enforcement, as there are multiple and distinct potential sources of attacks (both internal and external) as well as targets	Commercial espionage and hacktivism are two, albeit distinct, threats. There is little evidence that Brazil is impacted by the other types of threats in this category.
Emerging threats	Threats related to the expansion of cyberspace that do not fit well in the ITU categories, whether because they are emerging or are more related to the developing world.	ICTs used by more traditional criminal groups, like gangs and organized crime (drugs and arms trafficking, online extortion, spread of a culture of violence), cyber money laundering and tax evasion, etc.	It should be more linked to law enforcement, but this field is just emerging and there is still lack of state response	Brazil suffers from high levels of interpersonal and organized violence, especially related to gangs and organized crime profiting from drug trafficking. These have already learned the power of ICTs to expand and strengthen their businesses.

Conventional cybercrime

Like other real-world illicit activities, cybercrime is extremely difficult to measure with precision. Cyberspace is simply too vast and decentralized for researchers to gauge, track and report the entirety of malicious activity with certainty. Indeed, it is exceedingly difficult to even render an order of magnitude estimate of cyber-crime. This is because governments and companies are averse to releasing this sort of information for fear of reputational damage and loss of confidence and investment. Still, some state agencies and private cyber-security firms issue routine reports of the estimated size of cyber-criminal markets. Numbers and figures are, at best, rough approximations, leading to wide discrepancies in the projected impact of these markets. Even so, they offer some insights into broad trends that can help begin setting priorities and associated resource-allocation questions.

All available reporting indicates a significant increase in cyber-criminal activity in Brazil over the past decade. This rise coincides with the increased access to ICTs across the country from 2000 onwards. The total number of reported computer incidents received by CERT.br (Brazil's central Computer Security Incident Response Team or CSIRT), jumped from 6,000 in the year 2000 to more than 466,000 in 2012 [29] (see Figure 1). At least 75 per cent of Brazilian Internet users claim to have been victims of one form of cybercrime or another. The global average is 67 per cent, while the highest rates are found in Russia (92 per cent), China (84 per cent) and South Africa (80 per cent). With respect to the hacking of social network profiles, Brazil tops the ranking alongside China, with 23 per cent of users reporting having their accounts taken over by another user. At least 12 per cent of Brazilians claim to have had their PCs infected by malware through phishing schemes employing fake websites sent via social media.[30]

Figure 1. Total Computer Incidents Reported to CERT.BR annually (1999-2012)



[29] Total Computer Incidents Reported to CERT.BR annually (1999-2012). See http://www.cert.br/stats/incidentes/ (CERT.br keeps statistics on notification of reported incidents. These notifications are voluntary and reflect incidents that occurred in networks that spontaneously warned CERT.br).
[30] See http://oglobo.globo.com/tecnologia/brasil-perde-16-bilhoes-por-ano-com-ciberataques-6280831#ixzz2BZTx7kkV.

Cyber security companies also provide some insights into the extent of malicious digital activities in Brazil. Indeed, Brazil ranks number one in the LAC region as a source and target of online attacks. This applies to all manner of computer-related cyber-offenses including malicious code, spam zombies, phishing hosts and botnets, among others. These trends are increasing at an alarming rate. There has been a rapid escalation of cyber-crime in Brazil over the past decade, with most US and European security firms identifying Brazil as one of the world´s most problematic countries for cyber-crime activity since 2006.[31] Today, the principle cyber-crimes committed in Brazil include the spread of viruses or malware (68 per cent), hacking of social media profiles (19 per cent), and phishing (11 per cent).[32] Although Brazil reports considerable spam activity (3.4 per cent of global flows in 2012, a modest ranking in comparison with the chart leader, US with 42.2 per cent), these are decreasing dramatically and are no longer a serious problem among users.[33]

Bank fraud is something of a Brazilian specialty due in part to the sheer size of the country´s electronic banking service sector. The *Brazilian Federation of Banks* (Febraban) claims that the total losses to financial institutions in 2011 amounted to US$ 750 million. Febraban also observed a 60 per cent annual increase in bank fraud committed using the Internet and mobile phones, call center transactions and credit cards. A Kapersky Labs report in 2011 placed Brazil ahead of China and Russia in the use of Trojan horses to hack e-banking accounts: 16.9 per cent of the total annual attacks were launched against Brazilian users, as compared to 15.8 per cent in Russia and 10.8 per cent in China.[34] Even so, many of these frauds were committed offline, through telephone and credit/debit card scams (US$ 450 million). US$ 150 million was reportedly lost through Internet and mobile banking. Another US$ 150 million was stolen through digital payments of credit card bills.[35] In some areas, Brazil is ahead of North America and Western Europe in relation to digital security in the banking sector: for example, changing passcode systems, two step verification and biometrics are all standard.

Brazil is also a haven for other types of cybercrime identified by the International Telecommunications Union (ITU). Chief among these are those perpetrated against companies and business,[36] content-related offenses [37] and copyright and trademark offenses.[38] The overall costs of Internet crime in Brazil, including fraud and stolen

---

[31] See http://www1.folha.uol.com.br/tec/1143535-cibercriminoso-brasileiro-promove-ataque-sofisticado-a-banco-on-line.shtml.

[32] Ibid. In 2012, Brazil was ranked fourth in phishing attacks (4%), trailing only the US (29%), the UK (10%) and Australia (5%). Total losses that year through this kind of scam were US$ 10.5 billion. Source: See http://www1.folha.uol.com.br/mercado/1181392-ataques-ciberneticos-causam-perdas-de-us-21-bilhoes-a-empresas.shtml (RCA/EMC data).

[33] Spam statistics are generated through information acquired via complaints made to SpamCop and forwarded to CERT.br. See http://cetic.br/seguranca/index.htm and http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33298&sid=4#.UXpdF6LU_Io.

[34] See http://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml (Kapersky data).

[35] See http://info.abril.com.br/noticias/seguranca/brasil-perde-bilhoes-com-crimes-ciberneticos-04112012-13.shl.

[36] PricewaterhouseCoopers (PwC) determined that 32% of Brazilian companies are victims of some form of cybercrime each year. This is higher than the global average (23%). PwC found that 39% (the majority of affected businesses) suffered losses between US$100,000 and US$5 million. Roughly 5% had losses of up to US$1 billion. What is more, only 24% of Brazilian companies claimed that they could routinely detect and contain the leaking of sensitive data about their clients and suppliers. See http://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml (PricewaterhouseCoopers data) and http://www1.folha.uol.com.br/fsp/tec/90924-empresas-falham-na-protecao-de-dados-admitem-executivos.shtml.

[37] See Safernet website for data (http://indicadores.safernet.org.br/). Safernet is a Brazilian NGO that centralizes reports on content-related digital offenses in Brazil.

[38] Little is known about the scope and scale of this dark market in Brazil, but we can glean some information from the International Intellectual Property Alliance (IIPA), which in a recent report found that the Internet is the primary vector for piracy in Brazil and is growing exponentially. It added that this illegal activity causes "overall losses to the economy totaling US$4.16 billion". Around 1 billion songs are downloaded illegally in Brazil per year, not to mention other types of intellectual and artistic property. See IIPA "2012 Special 301 Report on Copyright Protection and Enforcement".

banking information, is about US$ 8 billion annually (or 7 per cent of the total global losses generated by cybercrime).[39] These estimates suggest that the country is the third most affected by illegal digital activities worldwide. In Latin America, Brazil is the number one target by a considerable margin: Mexico trails Brazil with annual losses of roughly US$ 2 billion due to cybercrime.

Complex cybercrime

Another category of cyber criminality consists of so-called *complex cyber-offenses* – especially threats to government institutions.[40] Their extent and nature in Brazil are still not at all clear. There is a lack of both quantitative and qualitative research shedding light on the scale of these "threats", though specialists are nevertheless worried. Instead, there are occasional anecdotal insights of complex offenses that can serve as an indication of wider phenomena. These offenses are typically of most concern to national, state and municipal governments, as well as the armed forces and, to some extent, law enforcement. They also inform and shape choices adopted by governments in relation to the formation of cyber security infrastructure. Those most concerned with complex cyber offenses often reproduce statistics and anecdotes that are repeated incessantly, but lack evidence or corroborating data. Three complex cyber-offenses deserve special attention.

First, in contrast to benign forms of digital activism, public authorities across Brazil view hacktivism with real suspicion. There is no clear understanding of the extent of physical and economic damages caused by hacktivists, whether as a result of government or private sector website defacement or denial of service (DDoS) attacks. The greatest concern to authorities is arguably the theft and release of sensitive official information. As the Assange and Snowden cases demonstrate, information obtained through these methods can be rapidly and efficiently published and disseminated online. In other cases, such information can be used as a bargaining chip, to extort and for blackmail. In Brazil, the government (the Presidency and numerous ministries, including Itamaraty, the Ministry of Foreign Affairs), the security forces (including the army and police units),[41] as well as private and public companies (Petrobras and banks such as Banco do Brasil, Itau and Bradesco), are regularly targeted by hacktivists.[42]

The most prominent hacktivist groups in Brazil are Anonymous and LulzSec, although the latter has purportedly called off its activities.[43] Because of a desire to preserve anonymity and a decentralized and non-hierarchical structure, participants of these groups are difficult to contact. When they do speak out, they justify their actions based on broad ideals,[44] such as their opposition to "widespread inequalities in Latin America" (when it comes to corporations and financial institutions) and "against widespread manipulation of information by

[39] See Norton/Symantec (2012) "Norton Cybercrime Report 2012" and http://www1.folha.uol.com.br/tec/1163431-custo-anual-do-cibercrime-no-brasil-e-de-r-16-bilhoes-diz-estudo.shtml.

[40] Complex or combined cyber offenses are defined by ITU as types of cybercrime that may fall within more than one category among the following: offences against the confidentiality, integrity and availability of computer data and systems; content-related offences; computer-related offences; and copyright- and trademark-related offences. See ITU (2009), pgs. 51-59.

[41] See http://www1.folha.uol.com.br/cotidiano/1211459-hackers-invadem-perfil-de-gcm-e-divulgam-dados-pessoais-em-rede-social.shtml.

[42] For a few other cases and examples, see http://www.bloggingsbyboz.com/search/label/cyber-security.

[43] See http://idgnow.uol.com.br/seguranca/2011/06/27/lulzsec-encerra-atividades-depois-de-50-dias-de-caos/.

[44] Indeed, during the 2013 Brazilian protests, Anonymous' local arm adopted a comparatively quiet posture with few clear objectives. See http://www.diariodocentrodomundo.com.br/o-ultrarreacionarismo-do-anonymous-do-brasil/.

authorities."[45] In other cases, hacktivists are more interested in conducting pranks and generating mischief. Hacktivist attacks were commonly reported in 2011 and the beginning of 2012 (more than 1,250 cases).[46] During 2012 and the beginning of 2013, however, the caseload dropped dramatically. Hacktivism tends to arise in specific situations, such as when a controversial bill is voted on in Congress. Not surprisingly, during the popular protests of mid-2013, there was a dramatic surge in hactivism that targeted powerful media outlets in the country including Globo and Veja.[47] FIFA's Confederation Cup and World Cup in 2013 and 2014 were also targeted.

Second, the Brazilian government is witnessing growing attacks against state systems and networks. Such threats are alarming to authorities, especially the federal public administration and the armed forces. The Department of Information and Communication Security (DSIC) of the Presidential Office for Institutional Security (GSI-PR) is responsible for the former and is charged with guaranteeing "the availability, integrity, confidentiality and authenticity" of information and communication in that sphere. Since 2009, DSIC's Director and Brazil's "cyber-security czar", Raphael Mandarino,[48] has repeatedly alluded to some 2,000 attacks launched every hour against the government´s 320 public federal networks. Although the origin of the attacks is rarely mentioned, Mandarino contends that 70 per cent involve efforts to retrieve banking information from public financial institutions.

Another 10 per cent allegedly target INFOSEG in the Justice Ministry, a closed network containing large amounts of data on criminal inquiries and prosecutions. An additional 15 per cent aim to retrieve the personal data of public servants.[49] General José Carlos dos Santos, former commander of CDCiber, has frequently drawn attention to the extent of attacks directed toward military networks, numbering some 30,000 per day.[50] Surprisingly, a considerable proportion (30 per cent) of these networks is managed by private ISPs and civilian networks,[51] a disconcerting revelation considering the sensitivity of military information. Notwithstanding the sheer scale of daily attacks perpetrated against these networks – many of them criminally and economically motivated – only two cases succeeded in leaking information to the public domain. [52]

The third complex cyber threat is cyberterrorism and cyber-warfare. The threat of terrorism is routinely invoked by governments and armed forces around the world to justify the securitization of a country's cyberspace. The US military, for example, has designated cyber as the fifth most important battle-space priority. In Brazil, two factors are frequently cited to justify the authorities' use of a hard cyber-security posture. The first is the protection of *critical national infrastructures* (CNIS). The revelations about the Stuxnet worm that targeted the

[45] See http://www.google.com/hostednews/afp/article/ALeqM5jyN0Fn4ZXfibMLdsclqXDnlXVDjw and http://itdecs.com/2011/06/brazil-suffers-its-biggest-cyber-attack-yet/.

[46] See Kishetri (2013), p. 145.

[47] See http://www.anonymousbrasil.com/brasil/twitter-da-veja-e-hackeado/ and http://www.tecmundo.com.br/Ataque-hacker/42249-Perfil-do-G1-no-Twitter-e-hackeado-por-ativistas.htm.

[48] See http://www.gsi.gov.br/sobre/quem_e_quem/quem_e_quem_secretaria_executiva.

[49] See http://info.abril.com.br/noticias/seguranca/redes-do-governo-tem-48-mil-ataques-por-dia-23082009-4.shl.

[50] See http://www.defesanet.com.br/cyberwar/noticia/1632/CDCiber---Na-guerra-cibernetica--Brasil-adota-estrategia-do-contra-ataque.

[51] See Canal Livre (TV show TV Bandeirantes Network, 29 July 2011. Available at http://www.youtube.com/watch?v=ID8N7y86Aow.

[52] The first leak involved unclassified and non-sensitive information. It included some personal data of soldiers working on social projects in the Northeast of Brazil. The second case involved the disclosure of personal details of names and addresses of Rio de Janeiro-based police officers during the 2013 protests. See http://www1.folha.uol.com.br/cotidiano/2013/09/1342381-hackers-invadem-site-e-divulgam-dados-de-50-mil-policiais-militares-no-rio.shtml

Iranian uranium enrichment facility in Natanz in 2010 generated major concerns in Brazil. Indeed, there was an array of baseless rumors circulating in Brasilia that a national power outage a few years ago was triggered by a similar attack.[53] With Brazilian energy officials unable to explain the reasons for the blackouts, cyber security experts recalled alleged cyber-attacks to the power grid in 2005 and 2007.[54] The protection of the CNIS against "external threats" is analogous in some ways to conventional deterrence theory. If authorities believe that the "enemy" can inflict real damages – even if the chances of such an attack occurring are minimal – then they will invest heavily to shore-up national defenses from prospective threats.

A particular concern of the Brazilian authorities is the exposure of its *mega events-related networks*. Brazil is hosting an increasing number of large-scale initiatives, including sporting events, international conferences and arts festivals.[55] These put major cities such as Brasilia, Rio de Janeiro and Sao Paulo in the global spotlight. CDCiber is responsible for protecting these networks. An example of this is CDCiber´s role in providing security for the UN Rio+20 Conference in 2012. The unit worked jointly with the Federal Police to protect networks from repeated attacks during the event.[56] While most of these incursions were launched by ordinary criminals, there were also attacks mobilized by hacktivist groups (e.g., Anonymous) and others seeking to obtain sensitive data.[57] CDCiber was also involved in coordinating cyber-security during the visit of Pope Francis to Brazil and FIFA's Confederation Cup (2013) and World Cup (2014). It is still an open question whether the threat of terrorism or a lone wolf attack warrants such a scaled-up response.

The fourth risk that is currently being used to ramp up the securitization of cyberspace is cyber-espionage. Brazil had no previously recorded cases of *cyber-espionage* from a foreign government before 2013. Indeed, there were no public reports even of industrial espionage before the emergence of Edward Snowden at around the same time as the digital and street protests in mid-2013. And yet the revelations of massive surveillance by the National Security Agency (NSA) in the US changed everything. According to a series of reports issued by the Guardian and other news outlets, millions of Brazilians' calls and e-mails were tapped by the NSA.[58] When it comes to the sheer extent of NSA-led cyber-surveillance, Brazil is second only to the US itself.[59] US intelligence officials allegedly rationalized this surveillance on the grounds that Brazil occupies a strategic position in managing global telecommunications infrastructure (i.e. transmission lines and optical fiber cables). Far from being enemies, they argued, the US was "protecting" this critical asset. Meanwhile allegations also emerged of the tapping of phones and emails of President Dilma Rousseff, Ministry of Energy officials and

53 News reports in the US never actually backed these claims with credible evidence.

54 The lack of accurate information about this case is striking. One document attributes the claim to a speech given by US President Obama in which he refers to the case but without naming Brazil: "We know that cyber intruders have probed our electrical grid, and that in other countries cyber attacks have plunged entire cities into darkness'. (…) It is now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation." See http://cii.in/WebCMS/Upload/Amaresh%20Pujari,%20IPS548.pdf.

55 Events include, for example, FIFA's Confederation (2013) and World Cup (2014) and the Olympic Games in Rio (2016).

56 See http://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html.

57 Anonymous launched operation #OPHackInRio during the Rio +20. See http://g1.globo.com/tecnologia/noticia/2012/06/anonymous-ataca-sites-ligados-ao-governo-em-protesto-contra-rio20.html.

58 See http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934.

59 See http://oglobo.globo.com/infograficos/volume-rastreamento-governo-americano/.

senior Petrobas executives,[60] leading to the cancelation of Rousseff's state visit to the US and recriminations in the UN.[61]

Of course, the Brazilian government is not entirely innocent when it comes to cyber espionage. At the same time as Brazilian authorities were expressing outrage about NSA-led surveillance, they were simultaneously authorizing ABIN and CDCiber – the entities responsible for protecting the country from precisely this type of interference – to monitor social media activity in Brazil related to the mass protests of June-August 2013.[62] ABIN has been criticized for not anticipating the events leading-up to the Brazilian protests in 2013. Even so, ABIN soon established and deployed a social media monitoring platform called Mosaico to track users and predict new events. The monitoring system is controversial to some Internet activists because it can lead to self-censorship and pressures on legitimate social movements.[63] The same applies to the program Guardião mounted by the military at CDCiber.[64] Nevertheless, Brazil is moving ahead to consolidate control over its cyberspace. The Brazilian government is developing a $185 million fiber-optic cable with Portugal to guarantee more autonomy over Internet traffic to and from the country.[65]

Emerging forms of cybercrime and gaps in knowledge

A serious challenge for governments and companies is anticipating and tracking down cyber threats. Threats are all about probability, whether they might exist and when and where they are likely to be deployed. Approaching these two dimensions critically can help clarify what institutions fail to see and also what they do not want to see due to stove-piped interests. There are a number of areas that warrant further reflection if only to broaden the debate on cyber malfeasance in Brazil. These are important to take in to account in order to challenge wrong-headed responses.

First, there is the question of who are the offenders. Cyber-security expert, Mikko Hypponen of F-Secure, contends that governments are losing the battle against cyber-offenders because they do not invest sufficiently in determining who they are. Nor are states especially attuned to their motivations, organizational characteristics or even the nature of their membership. Such knowledge is essential for the design of effective strategies to contain, manage, prevent and reduce cybercrime. Instead, there is a tendency to conflate categories of cyber-offenders, leading to a generic response to cyber-crime rather than an acknowledgment of the genuinely heterogeneous nature of criminal practices. Cyber-criminals regularly adapt their tools and practices to circumvent new cyber-defense mechanisms.

60 See http://noticias.uol.com.br/internacional/ultimas-noticias/2013/10/06/ministerio-de-minas-e-energia-foi-espionado-por-canadenses.htm.

61 President Dilma Rousseff urged the UN to take the lead in regulating the conduct of states when it comes to ICTs and declared that Brazil would "present proposals for the establishment of a civilian multilateral framework for the governance and use of the Internet and to ensure the effective protection of data that travels through the web" (see more details about this in section four). See full speech at http://gadebate.un.org/sites/default/files/gastatements/68/BR_en.pdf.

62 See http://www.estadao.com.br/noticias/cidades,abin-monta-rede-para-monitorar-internet,1044500,0.htm.

63 See https://protestos.org/2014/06/18/exercito-usou-software-guardiao-para-monitorar-redes-sociais/.

64 See http://www.bloomberg.com/news/2014-10-30/brazil-to-portugal-cable-shapes-up-as-anti-nsa-case-study.html.

In Brazil, the Federal Police has created a database of individuals who are being prosecuted for cyber-crime. With the passing of new Brazilian cybercrime legislation, this dataset will be enlarged to capture a wider range of cyber-offenses. Organizing and operationalizing this data is crucial. Instead of resorting to an indiscriminate dragnet, it can help inform and shape cyber-security strategies to mitigate specific threats. From the existing data, we already know certain things: Brazilian cyber-offenders are typically well educated upper-middle class males from 25 to 35 years old. However, this information is based on a relatively small sample of 177 people arrested on charges of cyber-fraud between 2010 and 2012.[66]

According to the Federal Police, there is no public record of attacks launched by foreign groups or individuals,[67] but such incursions are likely to increase. Due in part to the country´s continuous hosting of mega events, its growing middle class and the digitization of financial services, Brazilians will likely face increasing attacks from foreign cyber-criminals.[68] There is also evidence that since 2004, Brazilian cyber-offenders are stepping up their pursuits overseas.[69] Portugal and Spain have been the primary targets, though Brazilian cyber-criminals are turning their attention to a wider set of Portuguese and Spanish-speaking communities in the US, UK and throughout South and Central America.[70]

Through a series of recent revelations, the *modus operandi* of Brazilian hackers is gradually being understood. A former Brazilian hacker has described how cyber-crime groups tend to organize in groups of three to five people. They may be dispersed within a single city, a state, a country or even between several countries. Many of them may also tap into cybercrime forums in the Deep Web, the portion of the Internet that is not indexed by standard search engines. Such forums have begun to dissipate, however, due to infiltration by US and international law enforcement and intelligence authorities. There is often a key intermediary contact who liaises directly with organized criminal groups and who provides the funds for developing malicious code. There are instances of drug traffickers, for example, paying software programmers to develop illicit sites[71] in order to more freely market narcotics. A prominent example of this is SilkRoad,[72] though there are many others.

There is also growing awareness of the *migration of traditional organized crime to cyberspace*. Criminal gangs have shown an increased presence online – especially on social media sites. Drug traffickers and militia groups regularly publish evidence of their exploits and enemies on Facebook, Twitter and YouTube.[73] There are also often clips of so-called *funks proibidões* which glorify violence online[74] (see Figure 2). More ominously, organized crime groups are also adopting new technologies to expand not just drug, prostitution and human

66 See http://info.abril.com.br/noticias/seguranca/brasil-perde-bilhoes-com-crimes-ciberneticos-04112012-13.shl?2.

67 Interview with the former head of the Federal Police Unit for Combating Cybercrime URCC, Delegado Sobral. CERT.br reports that only 20% of attacks on systems and networks in Brazil origninate from abroad. This does not mean that the attacks are necessarily launched by Brazilians, who can use proxy IPs located outside the national territory.

68 Interview with Delegado Sobral.

69 See Glenny (2009).

70 See http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33454&sid=18#.UXpdBqLU_lo

71 The Deep Web is formed by a vast ecosystem of websites and communications that are not ordinarily catalogued by conventional search engines and which are often accessible only via proxy. Some estimates categorize it as 500 times the size of the "visible" or surface Net. See, for example, http://en.wikipedia.org/wiki/Deep_Web.

72 SilkRoad was reportedly taken down by a hacker in 2013. See http://www.bbc.co.uk/news/technology-22381046.

73 See http://www.vice.com/read/mexicos-drug-cartels-are-using-the-internet-to-get-up-to-mischief.

74 See, for example, http://www.youtube.com/watch?v=u2thkZZvy0s and http://www.youtube.com/watch?v=GtAGrAhnfu4.

smuggling networks, but also to intimidate, coerce and protect territory. Some have migrated to ATM-based crime – moving from tearing entire machines from their physical moorings to the more delicate practice of credit card skimming.[75]

Figure 2. Screenshots of Brazilian Youtube videos exalting gangs and organized crime

These images celebrate two large gangs in Brazil, the Comando Vermelho (Rio de Janeiro) and the PCC (São Paulo). There are allegations that these groups are in fact developing tighter ties. The photos are available at http://www.youtube.com/watch?v=u2thkZZvy0s and http://www.youtube.com/watch?v=GtAGrAhnfu4 (as of May 2013).

For their part, Federal Police and others are beginning to track the movement of organized crime and gangs online, including in large and intermediate sized cities. While there are only a small number of examples of citizen groups using crowd-mapping tools to track crime and victimization (due in large part to fear of retribution [76]), security agencies are investing heavily in predictive analytics and data fusion systems to anticipate trends and patterns of criminality.

A key concern for the Brazilian authorities is *money laundering*. Recent estimates suggest that laundering ranges between US$ 2.5 to 4 billion annually in Brazil.[77] Cyberspace facilitates the movement, layering and dispersion of funds anonymously. And while not considered a "major" cybercrime in Brazil, the issue is taken very seriously by the Federal Police and Ministry of Justice. For example, the government has desginated *technology laboratories against money laundering* (LAB-LDs),[78] which draw on digital tools for analysis, interpretation and investigation. These new technologies are being used to track white-collar crime such as tax evasion, but also more systemic money laundering activities.

75 Information was supplied by the Federal Police URCC during an interview.
76 See Muggah and Diniz (2013).
77 See Ollinger (2013).
78 See http://portal.mj.gov.br/main.asp?View=%7B25703EA7-216D-4E91-86F5-946D73D87497%7D&BrowserType=NN&LangID=pt-br&params=itemID%3D%7BB2986C24-DA6B-4348-B9CB-4EA6164801A5%7D%3B&UIPartUID=%7B2868BA3C-1C72-4347-BE11-A26F70F4CB26%7D and the National Strategy Against Corruption and Money Laundering (ENCCLA) from 2006: http://enccla.camara.leg.br/.

A major focus of Brazilian security institutions is protecting the integrity of CNIS. While systems such as SCADA [79] and others are effectively disconnected from the Internet, this does fully limit their exposure to attacks. Some Brazilian authorities acknowledge that the country's CNIS is less reliant on computer-controlled systems as compared to more developed countries,[80] paradoxically protecting its infrastructure from attack. While this may be an advantage in terms of cyber-security (precisely because there is less interconnectivity with other networks), the government downplays this, since it may signal weakness as an emerging power. In the meantime, another national plan for the protection of critical infrastructure is emerging that will be distinct from the existing Brazilian cyber-security architecture.[81]

The heavy hand of the state

Brazil is evolving a cyber-security infrastructure that leans heavily toward militarized and securitized priorities. In the process, it is focused narrowly on specific types of cyber-threats while patently ignoring others. These choices yield significant consequences for cyber-governance in Brazil. Indeed, the decisions adopted by public institutions influence the scale and reach of surveillance, questions of net neutrality, the protection (or lack thereof) of privacy and the rights of citizens to information. It is important, then, to consider how Brazil is developing its cyber-security architecture. What is more, it is critical to examine the norms and practices shaping cyber-governance in the country.

Brazil's institutional cyber-security architecture

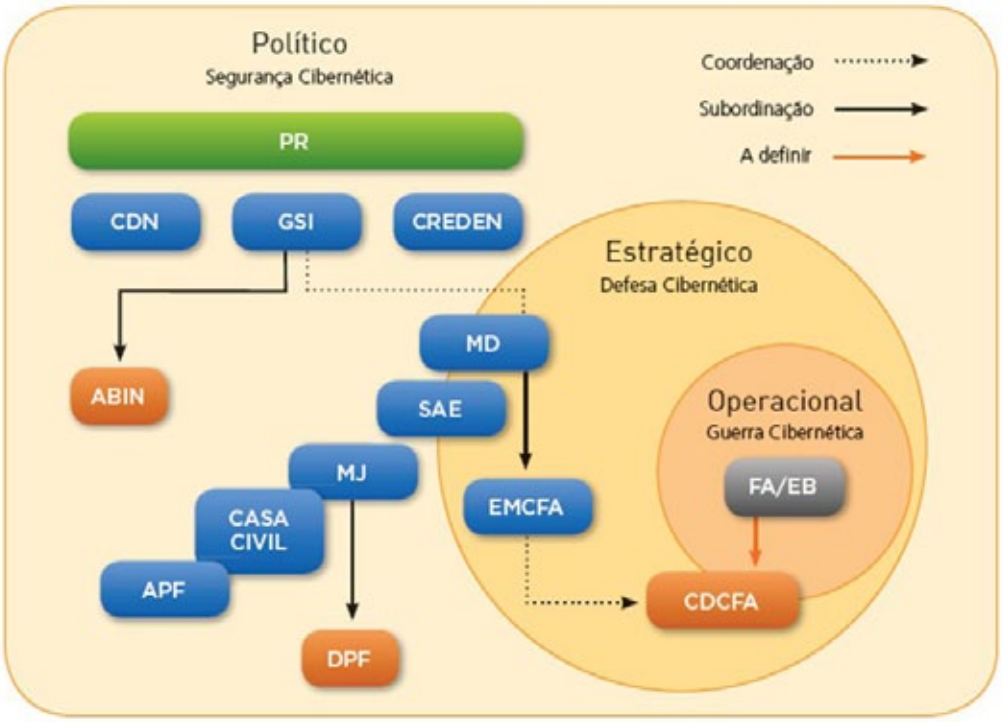
There is a multitude of public entities involved in managing cyber-security in Brazil. Many of them are focused exclusively on managing systems, technical development and upgrading tools. Examples include the Brazilian CSIRT (CERT.br), the Network Information Center (NIC.br, responsible for managing the country's top-level domain name), the Renato Archer's Center for Information Security, within the Ministry of Science and Technology, SERPRO, and INI, among many others. A smaller proportion is preoccupied with the cyber-security field as a whole. Depending on the agency, it may be involved in elaborating normative guidelines, adopting political decisions or authorizing action from national to local levels. Figure 3 below summarizes the principal actors operating at the federal level that are involved in shaping Brazil´s cyber-security architecture.

[79] SCADA is the acronym for "supervisory control and data acquisition". It is a computerized industrial control system, which can monitor and control mechanical processes that take place in industries and other facilities like the CNIS.

[80] Information provided by one of our interviewees. Brazil does not appear in a document prepared by TrendMicro, commissioned by the OAS CICTE, assessing the degree of "connectivity" of CNIS in Latin American countries. See TrendMicro (2013).

[81] A National Plan for Infrastructure Security is under development. Meanwhile, there is just one publicly available reference to how the government intends to protect critical information infrastructure written by DSIC: http://dsic.planalto.gov.br/documentos/publicacoes/2_Guia_SICI.pdf.

Figure 3. Brazil's cyber-security architecture: political, strategic and operational levels [82]



Accronyms from Figure 3:

PR: Presidência da República (Presidency)
CDN: Conselho de Defesa Nacional (National Defense Council)
GSI: Gabinete de Segurança Institucional (Presidential Office for Institutional Security)
CREDEN: Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (Chamber of Foreign Affairs and National Defense of the Council of the Government)
ABIN: Agência Brasileira de Inteligência (Brazilian Intelligence Agency)
MD: Ministério da Defesa (Defense Ministry)
SAE: Secretaria de Assuntos Estratégicos (Secretariat of Strategic Affairs)
MJ: Ministério da Justiça (Ministry of Justice)
APF: Administração Pública Federal (Federal Public Administration)
DPF: Departamento de Polícia Federal (Federal Police)
EMCFA: Estado-Maior Conjunto das Forças Armadas (Joint Chiefs of Staff of the Armed Forces)
CDCFA: Comando de Defesa Cibernética das Forças Armadas (Cyber-Defense Command of the Armed Forces)
FA/EB: Forças Armadas/Exército Brasileiro (Armed Forces/Brazilian Army)

There is a hierarchy of state institutions involved in managing Brazilian cyber-security. At the top of the pyramid is the *Presidential Office for Institutional Security* (GSI). In direct contact with the President, the GSI is a key government body tasked with dealing with all civil-related aspects of cyber-security. It is also responsible for other areas, including military affairs and cyber-defense (it is part of the *National Defense Council*, or CDN). Subordinate branches within the GSI include the *Department of Information and Communication Security* (DSIC), responsible for guaranteeing the availability, integrity, confidentiality and authenticity of information and communication for the federal public administration. This is coordinated in close consultation with the Civil House (Casa Civil), which is also responsible for overseeing the concession of digital security certificates (for key public infrastructure). Also within GSI are the *Secretariat of Strategic Affairs* (SAE) and the *Chamber of*

[82] See República Federativa do Brasil, Presidência da República, Secretaria de Assuntos Estratégicos (2011), p. 204.

Foreign Affairs and National Defense of the Council of the Government (CREDEN), an advisory commission to the President. The trio of DSIC, SAE and CREDEN are key players in shaping cyber-security debates in Brazil.[83]

Other institutions influencing Brazil's cyber-security agenda include the *Federal Police Department* (DPF), under the supervision of the *Ministry of Justice* (MJ). While its primary role is federal level law enforcement, it also has units devoted to cyber-security. Likewise, the *Brazilian Intelligence Agency* (ABIN), besides engaging in social media monitoring, has developed cryptographic competencies to protect public institutions. This is conducted through the Communications Security Research and Development Center (CEPESC). Finally, there is the Ministry of Defense (MD) that oversees the armed forces and serves as a liaison between civilians and the military. The role of the MD in shaping Brazil´s cyber-security architecture is analyzed in more detail in subsequent sections. Under the MD is also the Joint Staff of the Armed Forces (EMCFA), which also plays a role in coordinating cyber-response.

Normative responses to cyber-threats

Brazil is rapidly laying out national Internet and cyber-crime related legislation. There are more than 1,000 Internet-related bills currently under consideration by the Brazilian National Congress.[84] The *Marco Civil da Internet* is far and away the most important and widely known. The *Marco Civil* is a "Bill of Rights" for the Brazilian Internet and the first of its kind in the world.[85] It is a wildly popular initiative in Brazil and received significant support from Internet users during its initial drafting stages. It was developed through a participatory process, with contributions from all across the country. The Marco Civil establishes fundamental principles for the Internet, including freedom of speech, net neutrality and the protection of privacy. The bill was approved in April 2014 and is expected to strengthen and preserve user rights, which can in turn help counter-balance more nefarious practices that undermine user rights.

The National Congress was expected to approve the *Marco Civil* as far back as 2012, but controversies associated with two key issues resulted in the process being slowed down. The first of these controversies related to the question of *net neutrality*. Telecommunications companies attempted to obstruct and water down the principle of net neutrality by seeking to limit legal protections.[86] The second controversial area of the bill related to copyright infringements. Industries that depend on copyright being upheld demanded the power to require ISPs to remove illegal content without a warrant. And in spite of the opposition of telecoms and copyright industries, Congress acted to preserve net neutrality and impede the arbitrary removal of content (except for cases of revenge porn). Brazil is, perhaps not surprisingly, currently the world leader in requests for content removal from Google.[87]

---

[83] They have also recently developed a proposal for the elaboration of a long-term national cyber-security and cyber-defense strategy for the country.

[84] See http://observatoriodainternet.br/link-estadao-pls-de-internet-no-pais.

[85] See MCI website at http://edemocracia.camara.gov.br/web/marco-civil-da-internet.

[86] The telcom argument was that at the very least the "decrease in connection due to strictly technical reasons" should be explicitly allowed. See Le Monde Diplomatique Brasil, N. 65, December 2012.

[87] See https://knightcenter.utexas.edu/blog/00-13690-brazil-tops-googles-transparency-report-most-requests-censor-online-content

Another key element in shaping cyber-security presently being discussed within the *Marco Civil* framework is the so-called *log register.* The log register is a fundamental mechanism for cyber-investigation and related forensics. The question at stake during the aforementioned legislative deliberations was how long ISPs and content providers should be required to maintain "connection registers" so they could be reviewed by authorities. Some specialists argued that Brazil's telecommunications regulatory agency (ANATEL) should serve as the controlling body while others felt that the Congress should set the rules.[88] The latter prevailed, and the Brazilian Congress determined that ISPs must maintain data for one year, while content providers can hold on to data for up to six months. There were also concerns raised about the management of cyber cafes. On the one hand, they serve a critical function in terms of facilitating Internet access to low-income groups. On the other, they are also routinely used by cyber-criminals. In the end, the issue was not directly addressed in the *Marco Civil*.

While the original intention of the *Marco Civil* was to establish Constitutional guarantees and safeguards relating to the management of Brazil's cyberspace, it also became an impetus for aggressive cyber-crime prevention legislation[89] Indeed, Brazil´s first ever cyber-crime laws were passed due to popular outrage over a widely publicized hacking case, which involved the leaking of private photographs from the email account of a famous soap opera star.[90] An outcry from traditional and social media fueled the growing anxieties over the yet to be defined issue of digital privacy. Congress held an emergency session and passed a bill drafted in 2011 (and another that had been languishing since 1999). The first bill – which became law 12.373/12 [91] – has significant implications for Brazil´s cyber commons. A second bill – now law 12.735/12 – was so heavily amended that its likely effectiveness is questionable.[92] While some critics[93] contend that the legislation is confused and incoherent, the laws do successfully define and elaborate controls and punishments relating to Internet activity. For example, it is currently illegal to "to invade IT devices", "obtain private data", or "interfere or disrupt IT services".[94] Many points remain unclear.

It is worth noting that these most recent frameworks and laws were approved at a time when Brazilian officials started rethinking criminal justice legislation, which dates back to 1940. A new penal code will be voted on in the coming year and although it includes provisions to address cybercrime, these do not appear to resolve the contradictions and gaps in the existing laws.[95] There are an additional 40 bills related to fighting cybercrime awaiting approval in Congress.[96] The backlog reflects a widely known problem related to excessive legalism in Brazil's political system; it also highlights how the Brazilian government is still ill-equipped to respond to the dynamic and fast-changing cyber-crime landscape.

---

88 See http://www1.folha.uol.com.br/tec/2013/06/1295456-analise-rede-esta-virando-uma-ferramenta-de-vigilancia.shtml?utm_source

89 Brazil was one the last countries in Latin America to adopt a cybercrime legislation: see OAS REMJA website at http://www.oas.org/en/sla/dlc/remja/cyber_crime.asp

90 The star in question was Carolina Dieckmann from TV Globo in 2012.

91 See the integrity of the law at http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm

92 See http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm.

93 Interview with Walter Capanema. See http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33404&sid=4#.UXpc-KLU_lo

94 The cloning or theft of credit card data was already addressed by laws criminalizing the counterfeiting of documents.

95 Information provided by Walter Capanema during SEGINFO 2012 event (September). Available at: http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31777&sid=18.

96 Probably the most important issue for cyber-security is a bill that seeks to protect users' personal data. There is an expectation among activists that it will be a balanced law, one that protects privacy while strengthening and protecting important new services for the digital society, such as cloud computing and big data. See http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=33279&sid=11#.VGIoJjTF8ut

Law enforcement responses to cyber threats

Brazilian law enforcement and military entities are heavily investing in cyber-security activities on the ground. And yet there appears to be a disconnect between the types of threats affecting Brazilian cyberspace and the nature of the responses by security institutions. Organized crime is one of the major threats to Brazil's cyberspace, yet Brazilian resources are devoted disproportionately to military solutions better suited to the (rather rare) case of conventional warfare. There is less emphasis on expanding day-to-day law enforcement capabilities to identify and respond on organized crime groups. Due to the lack of a unified government position on the issue and the absence of reliable data, Brazil is developing an unbalanced approach to cyber-security. Instead, a small number of influential entities and individuals are shaping the debate in ways that will fundamentally determine the future of Brazil´s cyber-security architecture.[97]

The Federal Police's Unit for Combating Cybercrime (URCC) is the lead law enforcement agency responsible for preventing and responding to cybercrime. Its competencies range from the investigation of crimes against federal public institutions to infactions with inter-state and international ramifications. Given that cyber criminality invariably involves individuals and technologies spanning multiple states and actors beyond Brazil's borders, the Federal Police is an especially critical operational actor. It is involved in investigating electronic fraud (e-banking and credit card scams) and criminal networks promoting online child abuse. As a result of the aforementioned law 12.373/12, the Federal Police will soon be responsible for addressing unauthorized access of IT systems and networks.

The URCC, based in Brasília, also manages a cyber-intelligence apparatus [98] with teams deployed across most states. These are relatively small groups (the URCC itself has around 20 officers) and not necessarily composed of cyber-security experts. The URCC nevertheless coordinates all international law enforcement networks to facilitate the exchange of information and manage operational protocols. Moreover, the agency is connected to Interpol's Emergency Police Cooperation 24/7 and Ameripol; it can also leverage bilateral agreements for judicial cooperation. The URCC appears to be operating effectively in terms of exchanging information on operational matters with foreign law enforcement agencies and courts.[99] In contrast, when a case requires the cooperation of private Internet companies in the US, including Google and Facebook, there are often long delays and obstructions.[100] These companies tend to avoid collaborating with law enforcement due to contractual and legal obligations in the countries that host their core services and servers.[101]

The URCC has already undertaken operations against numerous cybercriminal groups including Trojan Horse, Matrix, Ponto.com, Liontech and Azahar.[102] In order to improve its investigative capacity, the Federal Police

[97] Two examples are worth mentioning including Raphael Mandarino Jr. (DSIC) and Gen. José Carlos dos Santos, former commander of CDCiber. The latter was replaced in 2014 by Gen. Paulo Sergio Melo de Carvalho.

[98] Centro Integrado de Inteligência Policial e Análise Estratégica da Polícia Federal (Cintepol).

[99] Authors' interview with Delegado Sobral (URCC-DPF).

[100] The Federal Police even arrested the President of Google's chapter in Brazil in 2012, after Google refused to take down a YouTube video that compromised a Brazilian politician (insight by Daniel Oppermann). For more info on the case, see: http://economia.ig.com.br/empresas/2012-09-26/presidente-do-google-no-brasil-e-preso-pela-policia-federal.html.

[101] US law enforcement agents routinely access data from companies registered in the US when in possession of a court order, giving the United States a significant strategic advantage.

[102] Azahar was an operation against a pedophilia network acting primarily through the Internet. The operation was carried out simultaneously in 30 countries in 2006. See http://idgnow.uol.com.br/mercado/2006/02/21/idgnoticia.2006-02-21.5692495488/.

implemented two projects, Tentacles (to filter and cross-reference data with an aim of reducing the number of processes to be assessed) and Oracle, designed specifically for the 2014 FIFA World Cup. Oracle consists of an intelligence-led predictive analytical system designed to assess future threats and provide basic information about would-be perpetrators.[103] The URCC also manages a Monitoring Center to track of suspicious digital activities. During the Rio+20 event in 2012, the URCC was able to merge the Monitoring Center with the cyber security wing of the Armed Forces, providing an additional layer of support. [104]

Law enforcement agencies in Brazil's 26 states and its federal district are becoming increasingly involved in engaging cybercrime at the subnational level. Officer Alexandre Wendt, has identified both opportunities and challenges confronting military and civilian police forces.[105] Wendt notes, on the positive side, the progressive establishment of specialized police units organized to address cybercrime over the past decade. Citizens and corporations are becoming more aware of these specialist units and in some cases are turning to them for assistance.[106] At the same time, Wendt worries that the police exhibit weak investigative and forensic capability.[107] Problems range from the lack of technical infrastructure and financial resources to poorly trained personnel, limited cooperation between law enforcement agencies and continued reticence of private firms to disclose the extent of cyber-crime. Challenges remain, notably the lack of standardization in evidence gathering and forensic procedures, as well as a limited capability to gather cyber-intelligence. Finally, there are open questions about how to manage cyber-crime in a complex federal structure in which it is remains unclear who is responsible for leading investigations or managing trials.

Armed forces responses to cyber threats

The extent of military preparation for cyber-warfare is not commensurate with the likely threat of armed conflict. Indeed, Brazil has not been involved in a war on its own territory since 1870 and has never been a target of international terrorism.[108] Nevertheless, the Brazilian government is preparing the armed forces to assume a leading role in the protection of Brazil's cyberspace, even though its primary use is civilian. There has been sizeable investment in upgrading military cyber capabilities – certainly more so than in the law enforcement sector. And while many other major powers are pursuing a similar approach,[109] the extent of Brazilian military involvement in cyber affairs is neither appropriate nor inevitable. In Latin America, where authoritarianism was the rule from the 1960s to the 1980s, only Colombia has encouraged the role of the armed forces in these areas to a similar degree as Brazil.

---

[103] See http://www.sagapolicial.com/2012/01/saiba-mais-da-pf-projeto-oraculo.html.

[104] Noted by Clayton da Silva Bezerra during SEGINFO 2012 event (September). Available at http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31793&sid=18#.Ue3JyI21HNw.

[105] Noted by Alexandre Wendt during SEGINFO 2012 event (September). Available athttp://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=31750&sid=18#.Ue3JhY21HN.

[106] It is important to note that Brazil's civilian state police forces were at the center of controversy during the Brazilian protests of 2013. For example, Rio de Janeiro's police unit specializing in cybercrime (DRCI) preemptively arrested protesters who were planning street demonstrations. See http://oglobo.globo.com/rio/doze-ativistas-deixam-complexo-penitenciario-de-bangu-na-madrugada-desta-quinta-feira-13284027.

[107] Brazilian police cannot rely on sting operations, since these operations are not regulated by the government (so they prefer to avoid taking risks) [Insight from Delegado Sobral]. Sting operations are a fundamental activity for the pursuit of cyber-criminals elsewhere (see Glenny, 2011).

[108] The country endured 21 years of military dictatorship (1964-1985), a period characterized by systematic abuses of human rights on the part of state agents.

[109] USA, France, Israel, UK, Russia and China, for example.

There are several reasons why Brazil is pursuing a military-centered cyber-security and defense architecture. For one, the armed forces are making a serious bid to expand their role as a key actor in shaping the direction of Brazilian affairs. While Brazil's democratic system continues to mature, the military is also being restructured and is seeking a new role in Brazil's domestic and foreign future.[110] This means shifting attention to emerging trans-border threats (including cybercrime) and engaging in internal security operations. This growing influence of the armed forces in civilian affairs has yet to be subjected to much domestic scrutiny. Indeed, Brazil´s armed forces enjoy unusually high support from the population. In spite of Brazil's history with military dictatorship, the armed forces are regarded by a majority as the most trusted national institution.[111]

At least part of the reason why there has yet to be much debate on the role of the Brazilian armed forces in cyber-security is that much of their activities are shrouded in secrecy. There is no public record or information detailing when the army first started developing its operational capacities in cyberspace. It was not until 2008 that the cyber field was officially incorporated into military doctrine. That year, cyber was designated one of the three main pillars for a renovated military, along with aerospace and nuclear power.[112] Since then, the Ministry of Defense has invested significant resources in the area. It also recently launched Brazil's Cyber-Defense Policy, a document containing the principles, objectives and guidelines that will guide its activity in this domain in the coming years.[113] The Ministry of Defense named the Army as the lead in developing cyber defense capabilities (the Navy is responsible for nuclear, while the Air Force has aerospace under its purview).

Figure 4. Different uses of cyber capabilities by the Brazilian Armed Forces

Source: Ministério da Defesa do Brasil - photos by Jorge Cardoso

Specifically, the Army was given control of an apparatus overseeing civilian affairs: CDCiber. CDCiber was created in 2010 and became operational at the end of 2011. CDCiber was created to coordinate the cyber-defense actions. As noted above, CDCiber is located between the strategic and operational levels of Brazil's cyber-defense architecture, coordinating with the MD, which in turn follows GSI-PR orders. This strategy includes cyber-activities in five core areas: Intelligence, Science and Technology, Operational ability, Doctrine and Human Resources.[114] CDCiber's principal objective is to provide protection to military and governmental

110 Consult http://g1.globo.com/brasil/noticia/2012/08/em-transformacao-exercito-planeja-estar-totalmente-equipado-em-10-anos.html.
111 See http://fgvnoticias.fgv.br/node/2847.
112 See National Strategy of Defense (END) from 2008.
113 The contents of the document can be found at http://www.defesanet.com.br/cyberwar/noticia/9128/MD---Politica-Cibernetica-de-Defesa.
114 Brazil is also to establish a National School for Cyber-defense, at a cost of US$20 million.

networks, from both internal and external attacks. Eventually, it will aim to protect the integrity of the national informatics infrastructure. CDCiber has at its disposal a cyberwarfare simulator, a laboratory for analysis of virtual malicious code and nearly one hundred officers trained in cybersecurity.[115] CDCiber is likewise expected to manage security during international mega-events and is consistent with Brazilian legislation mandating the deployment of the armed forces to guarantee the security of official and public events, "particularly those that anticipate the participation of Heads of foreign governments/states."[116]

Balancing threats and responses

A key question is whether the response of the Brazilian state to cyber threats is commensurate with the associated risks. There are some concerns that the military and law enforcement response may not only be disproportionate, but may also potentially undermine hard-won civil liberties. There are a number of reasons for the strengthening of cyber threat capacity, and not all of them have to do with the tangible threats on the ground. Rather, Brazil is using alleged cyber threats to reinforce its own domestic capabilities and extend its geopolitical influence. There are several risks associated with Brazil´s current approach.

First, Brazil's cyber-security architecture establishes clear competencies for its main actors in a field that is inherently ill-defined. In theory, the Federal Police is responsible for addressing common criminality (including investigation) and the army is supposed to be preparing for cyber-warfare (including defending national cyberspace from cyber-war and cyber-terrorism and formulating offensive actions when necessary). The issue of attribution, however, remains extremely difficult in cyberspace. It is still often impossible to determine with absolute certainty who or what is behind a serious cyber-criminal act, identifying where it originated or the underlying motives of the perpetrators. Indeed, cyber criminals are frequently recruited by governments for a wide range of activities. This may lead to the army becoming involved in situations where, legally and operationally, it has no business. It also underlines why inter-agency cooperation – especially intelligence – is critical.

Second, the security discourse of the agencies involved in cyber-security and cyber-defense initiatives is intrinsically biased. Most security entities contend that all the above-mentioned cyber risks are very real, dangerous and imminent. Many military actors refer to "ungoverned spaces" and the "Wild West" when describing cyberspace. These terms are typically accompanied by assertions of the need to conquer and control this space.[117] For example, General. José Carlos Santos, former commander of CDCiber, has noted that it may be possible for the Army's cyber-intelligence to be used to inform other authorities about "suspicious movements and mobilization around social protest that could disturb public order…"[118] As we observed,

115 See http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291,0.htm.

116 See Decreto N. 3.897 from 2001 at http://www.planalto.gov.br/ccivil_03/decreto/2001/d3897.htm.

117 These claims are noted in the República Federativa do Brasil, Presidência da República, Secretaria de Assuntos Estratégicos (2011). See, for instance, pages 16, 31 and 32.

118 See http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html.

this was the case when CDCiber and ABIN started the systematic monitoring of social media use in Brazil through the programs Guardião and Mosaico. Given Brazil's recent experiment with authoritarianism, this sort of rhetoric and practice leaves many feeling uneasy. This becomes even more problematic considering that in the near future the military may have access to civilian data. Indeed, the government recently announced that federal public administration networks will come under the purview of CDCiber, something that for the moment is the responsibility of a civilian department, DSIC.[119] These developments raise still more concerns in relation to the democratic control of the armed forces and wider rights to privacy.[120]

Initiatives are being designed and implemented without a clear, unified or predictable strategy. All official documents offering prescriptions or guidance on cyber-security are descriptive rather than prescriptive. Of special note is the *Green Paper for Cyber-Security in Brazil* (2010) and *SAE Strategic Challenges for Cyber-Security and -Defense* (2011). [121] The *National Strategy of Defense* (2008), for its part, is still unclear as to how cyber-security should be integrated into an overall strategy, even as the document elevates cyber as the central pillar of the Brazilian military establishment in the twenty-first century. The *White Paper for National Defense* (2012b)[122] should shed some light on these issues but is awaiting approval from the President´s office. The existing *Cyber-Defense Policy* of the Ministry of Defense only establishes rudimentary principles, objectives and guidelines for the consolidation of cyber specifically within the defense sphere.

Scarce resources are regularly diverted from core priorities and are inappropriately spent. Although the primary threats to Brazil's cyberspace are arguably related to economic crime and should result in corresponding increases in resources allocated to police entities, the armed forces are receiving the bulk of support.[123] For example, in addition to start-up costs, CDCiber received US$ 60 million in 2012 [124] and will receive another US$ 200 million through 2015.[125] According to estimates featured in Brazil's *White Paper National Defense*, the expected budget for cyber-defense is roughly US$ 420 million through 2035, which is actually a small proportion of the entire military budget projected for the period.[126] There are also legitimate concerns that

---

119 See http://www.estadao.com.br/noticias/nacional,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291,0.htm.

120 See http://oglobo.globo.com/pais/exercito-monitorou-lideres-de-atos-pelas-redes-sociais-9063915.

121 The Green Book of Cyber-Security (2010) was created by a working group under GSI. It lays out what it considers the key aspects of cyber-security in Brazil (see more in footnote 161). "Strategic Challenges for Cyber-Security and Defense" (2011) is the outcome document of a high-level conference organized by the Secretary of Strategic Affairs of the Presidency (SAE). It includes contributions from Brazilian experts and authorities in the cyber-field.

122 The White Book of National Defense is the first of its kind in Brazil. It was produced following consultations within government, but also in conjunction with civil society. It covers all aspects of national defense policy and articulates the long-term strategic vision of the armed forces.

123 The total amount devoted to law enforcement is not known. Even so, there are indications from key informants that the value of investment for police is far below what is being committed to the armed forces. Support for the police is difficult to quantify, owing to the way resources are distributed to many local police forces.

124 In 2012 R$ 5 million was also allocated for a simulation software application (developed by a Brazilian company). This is part of the strategy to integrate cyber-security with broader development concerns in the country as proposed by the Brazilian Green Book on cyber-security. See República Federativa do Brasil, Gabinete de Segurança Institutcional, Departamento de Segurança da Informação e Comunicações (2010). See also http://g1.globo.com/brasil/noticia/2012/08/em-transformacao-exercito-planeja-estar-totalmente-equipado-em-10-anos.html.

125 See http://www.tecmundo.com.br/tecnologia-militar/37801-exercito-deve-receber-r-400-milhoes-para-prevencao-de-guerra-cibernetica-.htm.

126 See República Federativa do Brasil, Ministério da Defesa (2012b) .

127 Even if the military receives more funding than law enforcement agencies, this does not necessarily imply it is adequate. Brazil is a serious power and should be able to afford to engage with international cyber security issues (that are not bounded by geography) and strengthen its response to genuine domestic issues. Out of a total defense budget of US$ 30 billion (2012-2015), the US$250 million specific budget for cyber is miniscule in relation to existing cyber-threats. See http://g1.globo.com/jornal-da-globo/noticia/2013/07/governo-destina-baixo-orcamento-para-seguranca-cibernetica.html.

the way in which these funds are being spent is inefficient and ineffective.[127] Recent revelations showed that Brazil's budget for 2012 was not spent in its entirety [128] and was mostly used for constructing CDCiber facilities.[129] The amount allocated to developing technologies, building capacities and training personnel was minimal. The reason given by the Minister of Defense is that "spending US$ 50 million in cyber-defense nowadays means that Brazil will have to buy foreign technology."[130]

Projecting soft power internationally

A key factor influencing Brazil´s investments in cyber-security is its desire to position itself as a global player on matters of international peace and security. Brazil's relatively recent emerging power status is creating a real impact domestically. In its attempts to assert itself internationally, Brazil is strengthening its still hard – or military – power apparatus. Brazil is also purposefully beginning to leverage its soft power – using civilian capacity – abroad. For example, Brazil is seeking to highlight successful domestic policy initiatives across key areas in pursuit of geopolitical influence. Cyber-governance and cyber-security are new and, in the vernacular, sexy, areas to exploit. They also have the advantage of being relatively inexpensive when compared, for example, with expanding military or peacekeeping capabilities. Cyberspace is also still an evolving area, allowing new entrants to take pioneering steps and guide multilateral agendas.

There are a number of claims Brazil can make with regard to its bolstering of hard and soft power capabilities in cyberspace. For example, CDCiber is the first dedicated military cyber-unit in Latin America. The Federal Police URCC's, while nascent, offers a model for law enforcement and judicial cooperation within and between countries and regions. Brazil can also boast about the development and application of cyber-security strategies designed for mega events. Moreover, Brazil might soon have the world's most comprehensive national cyber security and defense strategy. Perhaps most significant, Brazil has created the first digital Bill of Rights [131] and launched a UN initiative to promote digital sovereignty. All of these activities, while not necessarily internally coherent or coordinated, suggest that Brazil is staking out a claim in shaping the international and regional agendas on cyber-security.

At the same time, the Brazilian authorities have actively criticized and sought to reshape the existing cyber-security regime. For example, the government has criticized the Council of Europe's Convention on Cybercrime (the Budapest Convention of 2001) which, to date, is the only international legally-binding set of norms governing issues related to cyber-crime. Brazil argues that the drafting process deliberately excluded non-members of the Council and is thus biased against countries outside the European Union. In the meantime, Brazil has taken the lead together with UNODC to draft an international convention on cybercrime, receiving the support from other Latin American and Caribbean countries. The decision was taken during the 12th UN Congress on Crime Prevention and Criminal Justice held in Salvador, Brazil, in 2010, though the process is moving slower than its supporters had hoped.[132]

---

[128] One media source pointed out that just 8.9% was spent from the budget for 2012. See http://noticias.terra.com.br/brasil/brasil-usou-89-do-orcamento-para-defesa-cibernetica,76b782fb0acdf310VgnVCM3000009acceb0aRCRD.html.

[129] See http://www.bloggingsbyboz.com/2013/07/brazils-cybersecurity-budget-is-mess.html.

[130] See http://www1.folha.uol.com.br/mundo/2013/07/1312345-gastar-r-100-mi-em-ciberdefesa-significa-comprar-tecnologia-de-fora-diz-amorim.shtml.

[131] This includes a special acknowledgement by Tim Berners Lee recently. See http://www1.folha.uol.com.br/poder/2013/05/1280037-criador-da-web-elogia-brasil-por-projeto-que-vai-regular-a-internet.shtml.

[132] See http://www.stlr.org/2010/03/a-global-convention-on-cybercrime/.

There are also concerns with how Brazil is engaging global discussions on digital sovereignty and the potential for the Balkanization of the Internet. For example, Brazil sided to some extent with China and Iran during the ITU International Conference in Dubai (2012). Brazil favored the idea of regulating the Internet with an international treaty under UN supervision. There are concerns, however, that such an approach would confer excessive power to governments and lead to potentially cumbersome, restrictive and intrusive regulation. These concerns are heightened by the fact that the US and the US-based Internet Corporation for Assigned Names and Number (ICANN) control of the Internet is loosening to allow other governments, NGOs and ISPs to play a more prominent role. What is more, the ITU has raised prospect of permitting deep package inspection (DPI), the first step toward censorship and already applied in some countries.[133] More promising, however, there are signs that Brazil´s approach may be changing. Together with Germany and ICANN, the Brazilian government recently hosted a high-level event called NetMundial in Sao Paulo. Brazil proposed establishing a global "Marco Civil" and called for more *multistakeholderism* in relation to Internet governance.[134]

At the regional level, Brazil is collaborating closely with efforts to combat cybercrime coordinated through the Organization of American States (OAS) and its *Comprehensive Inter-American Strategy to Combat Threats to Cyber-Security* (adopted by the OAS General Assembly in 2004). Brazil has not only adopted the pillars for cyber-security outlined by the OAS but is working hard to improve on these proposed measures. The country has hosted conferences with the three OAS departments managing the implementation of the Strategy and frequently deploys government experts to support technical assistance missions and participate in events across Latin America and the Caribbean.[135] In its own neighborhood of South America, Brazil is pushing the agenda within the Union of South American Nations (UNASUR). Meetings of the Defense, Justice and Interior Ministers of the 12 member states have focused on the creation of mechanisms to enhance cooperation against transnational organized crime, especially cyber-crime.[136]

Brazil is also taking the lead in developing bilateral cooperation to manage cyber-security and cyber-defense. In 2010, it signed an *Agreement on Non-Aggression* by Information Weapons with Russia, the first such bilateral agreement anywhere. In addition to developing a non-aggression pact, the agreement calls for enhanced information exchange, capacity strengthening and joint cyber-warfare exercises. While the agreement is a curious one, there are signs of increased cooperation on cyber-security among BRICS members.[137] Meanwhile, the Defense Ministers of Argentina and Brazil also signed a 2011 Joint Declaration to review bilateral cooperation across the defense sector, including in relation to informatics and cyber-defense. Likewise, Defense Ministers from Brazil, Chile and Colombia have held closed sessions with the US Pentagon to review cyber threats and requested support to strengthen the resilience of hardware and software networks against breaches.

---

133 See http://www1.folha.uol.com.br/colunas/ronaldolemos/1210826-brasil-se-alinha-a-china-e-ira-em-leis-da-internet.shtml Brazil's position specifically on DPI is still unclear.

134 For more information on the event's outcomes, see http://netmundial.br/.

135 See Diniz and Muggah (2012).

136 See http://www.unasursg.org/index.php?option=com_content&view=article&id=516:ultima-unasur-debate-cooperacion-regional-en-crimen-trasnacional-organizado-y-nuevas-amenazas&catid=66:noticias-unasur.

137 See http://www.scmp.com/news/china/article/1276995/brics-emerging-economies-expand-co-operation-internet-security.

Conclusions

Brazil is doubling down on its cyber-security architecture while simultaneously consolidating its emerging power status. Public authorities are focusing not just on domestic cyber-criminality and cyber-activism but also expanding the state´s capability to mitigate cyber threats internationally. A central pillar of Brazil´s strategic response to both kinds of risks is CDCiber. And yet the emphasis on a militarized response may be incommensurate with the real (as opposed to existential) threats facing the country and society as a whole. The fact is that Brazil has comparatively few external cyber threats from foreign governments or terrorist groups. And yet, the rise of digital protest and cyber criminality is patently obvious, but receiving comparatively less attention and investment. There is an urgent need for a more informed and evidence-based reading of the threats confronting Brazil and engaging them with a careful consideration of balancing public safety and individual rights.

Brazil´s cyber security architecture is still evolving. There are still conflicting lines of accountability among institutions, distorted funding priorities, confused public debate, contradictory legislative measures and the uncritical importation of foreign solutions for local challenges. There are some critics that contend that the state´s "response" to cyber threats are misguided, and not aligned to the real challenges facing the country. Instead, the military has "captured" resources for cyber defense, with potentially dangerous implications for civil liberties more generally. The lack of coordination between government institutions and the fragmentation of responses is another major challenge. What is more, the limited engagement of civil society in cyber security debates in Brazil means that the armed forces have free reign to advance their corporate interests.[138] Instead, they tend to also adopt compartmentalized approaches, with some focused on issues of defense, others on policing, and still others on digital sovereignty, civil liberties, and the like. What is needed is a balanced cyber security strategy that accurately gauges evolving threats, but also elaborates proportionate and forward-looking responses.

A first step is to focus on filling knowledge gaps. There is a lively conversation in Brazil about the many positive developments related to e-governance, smart cities, digital sovereignty and other new ICTs.[139] Curiously, there is a silence on issues related to cyber-security and cyber-defense. Where debated at all, conversations tend to be reserved to the highest levels of government, the armed forces, law enforcement bodies and a narrow bandwidth of academia. If Brazil is to develop a more balanced and proportional response to actual and emerging threats, cyber-security must be recognized as an integral feature of cyber-governance and a key determinant of civil, social and political rights. At a minimum, Brazilian scholars need to begin better understanding the dynamics of hackers and cyber-crime groups, the ways in which traditional crime is migrating online, the ways in which security forces are adapting new surveillance technologies and other issues. But it also means that government should encourage a broader debate with a clear communications strategy about the need for cyber security and what forms this might take.

138 For an overview of how civil society engages with cyber-security in Latin America, see Diniz and Muggah (2012).

139 See, for instance, the works of research groups like ITS-Rio, CTS-FGV, UFABC (Research group "Cultura Digital e Redes de Compartilhamento") and UNICAMP (Research group "Políticas Públicas de Acesso à Informação").

The second step is to begin debating the content of measured and efficient strategies to engage cyber threats. Since the budgets allocated for cyber-related issues are flexible and hard to predict, there is considerable bureaucratic competition over funds. Military, law enforcement and civilian entities may exaggerate risks so as to increase their likely access to resources. A more informed negotiation could contribute to a more balanced cyber-security portfolio. Key priorities for Brazil include improving the investigative capacities of the federal and state police, including in relation to cyber forensics. Likewise, improved coordination between state police forces to anticipate and respond to cyber-crime is exceedingly important. Perhaps more radical, but a strategy pursued in other countries, is identifying and recruiting skilled Brazilian hackers to help upgrade state capabilities. The Brazilian Minister of Science and Technology has already made gestures in this direction, inviting hackers to evaluate the risks to the federal government´s network security. CDCiber has also made similar moves in this direction.[140] And yet Brazil's cyber-security czar has instead determined that all hackers are criminals (and that Brazilian hackers are not as skilled as their foreign counterparts).[141]

Third, Brazil must initiate a sophisticated debate on what constitutes cyber threats and the types of responses that are warranted. There is a tendency to oversimplify the discussion of cyber threats and cyber-crime. In some cases various types of activities are conflated. In others, there is a tendency to over-focus on a specific category of threat. If Brazil is to adopt a more progressive approach, a greater emphasis is needed on upgrading the quality of education and debate. The fact is that awareness about cyber security is exceptionally low in Brazil.[142] A concerted effort is required to raise understanding and engagement, as is the case in North America and Western Europe, among other places. Such a discussion should be open to multiple interests and based on solid empirical data. If Brazil is to build a cyber security architecture fit for purpose, a qualified debate is imperative.

[140] See http://revistaepoca.globo.com/Revista/Epoca/0,,EMI249428-15223,00-GENERAL+JOSE+CARLOS+DOS+SANTOS+PODEMOS+RECRUTAR+HACKERS.html.

[141] See http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27324&sid=21 and http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=27454&sid=15#.UaKzStLU-Io.

[142] About 42% of Brazilians reportedly do not know that computer viruses can persist unnoticed (global average is 40%). See Norton/Symantec "Norton Cybercrime Report 2012".

References

Canongia, C. and Mandarino, R. (2009). "Segurança cibernética: o desafio da nova Sociedade da Informação". *Parceria Estratégica.* Brasília-DF, vol. 14, n. 29, p. 21-46, jul-dez

Diniz, G. and Muggah, R. (2012). *A Fine Balance: Mapping Cyber-(In)security in Latin America.* Strategic Paper 2. Igarapé Institute: Rio de Janeiro, June. Available at http://igarape.org.br/a-fine-balance-mapping-cyber-insecurity-in-latin-america/

FGV-CPS (2012a). *Mapa da Inclusão Digital.* Marcelo Neri (Coord). Rio de Janeiro. Available at: http://www.cps.fgv.br/cps/telefonica/

FGV-CPS (2012b). *O Início, o Fim e o Meio Digital: Cobertura, Capacidades e Conectividade.* Marcelo Neri (Coord). Rio de Janeiro. Available at: http://www.cps.fgv.br/cps/vivo/

Glenny, M. (2011). *Dark Market: Cyberthieves, Cybercops and You.*

Glenny, M. (2009). *McMafia: A Journey Through the Global Criminal Underworld.* New York: Random House.

International Intellectual Property Alliance – IIPA (2012). *Special 301 Report on Copyright Protection and Enforcement: Brazil.* February. Available at http://www.iipa.com/rbc/2012/2012SPEC301BRAZIL.PDF

International Telecommunication Union (2009). *Understanding Cybercrime: A Guide for Developing Countries.* Geneva: ITU-D ICT Applications and Cybersecurity Division.

Kishetri, N. (2013). *Cybercrime and Cybersecurity in the Global South.* Palgrave MacMillan: United Kingdom.

Muggah, R. and Diniz, G. (2013). "Using Information and Communication Technologies for Violence Prevention in Latin America". In Mancini, F. (ed.) *New Technology and the Prevention of Violence and Conflict.* New York: International Peace Institute, April. Available at: http://www.undp.org/content/dam/undp/library/crisis%20prevention/20130410NewTechnologyandPreventionofViolenceandConflictv2.pdf

Norton/Symantec (2012). Norton Cybercrime Report 2012. Available at http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

Ollinger, M. 2013. "La Propagación del Crimen Organizado en Brasil: Una mirada a partir de lo ocurrido en la última década". In Garzón. G. and Olson, E. (eds) La Diáspora Criminal: *La difusión transnacional del Crimen Organizado y cómo contener su expansión.* Woodrow Wilson International Center for Scholars – Latin America Program. Washington D.C. http://www.wilsoncenter.org/publication/CriminalDiaspora

República Federativa do Brasil, Gabinete de Segurança Institutcional, Departamento de Segurança da Informação e Comunicações (2010). Livro Verde da Segurança Cibernética no Brasil. Mandarino, R. and Canongia, C. (Eds). Brasília. Available at: http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf

República Federativa do Brasil, Ministério da Defesa (2008). *Estratégia Nacional de Defesa.* Available at http://www.mar.mil.br/diversos/estrategia_defesa_nacional_portugues.pdf

República Federativa do Brasil, Ministério da Defesa (2012a). "Política Cibernética de Defesa". Portaria Normativa No 3,389 (December 21st), Gabinete do Ministro. DOU Seção 1 – No. 249 (December, 27th).

República Federativa do Brasil, Ministério da Defesa (2012b). *Livro Branco de Defesa Nacional.* Brasília. Available at: https://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf

República Federativa do Brasil, Presidência da República, Secretaria de Assuntos Estratégicos (2011). Desafios Estratégicos para a Segurança e Defesa Cibernética. Brasília, 1ª edição. Available at http://www.sae.gov.br/site/?p=6151

Trend Micro (2013). *Latin American and Caribbean Cybersecurity Trends and Government Responses.* May. Available at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-latin-american-and-caribbean-cybersecurity-trends-and-government-responses.pdf

Wæver, O. (1995). "Securitization and Desecuritization." In Lipschutz, R. ed. *On Security*. New York: Columbia University Press.

OTHER PUBLICATIONS BY IGARAPÉ INSTITUTE

STRATEGIC PAPER 10

Digitally Enhanced Child Protection: How New Technology Can Prevent Violence Against Children in the Global South

Helen Moestue and Robert Muggah

(November 2014)

STRATEGIC PAPER 9

Promoting Gender and Building Peace: The Brazilian Experience

Renata Giannini

(September 2014)

STRATEGIC PAPER 8

Making Brazilian Cities Safer – Special Edition of the Citizen Security Dialogues

Citizen Security Dialogues

(August 2014)

STRATEGIC PAPER 7

Changes in the Neighborhood: Reviewing Citizen Security Cooperation in Latin America

Robert Muggah and Ilona Szabó

(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

Securing the Border: Brazil's "South America First" Approach to Transnational Organized Crime

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)

The Igarapé Institute is a southern think tank devoted to evidence-based policy and action on complex social challenges. The Institute's goal is to stimulate humane engagement on emerging security and development issues. The Institute's approach is to: diagnose challenges through cutting-edge research; trigger informed debate and action across public and private spheres; design tailor-made solutions that are people-centered. The Igarapé Institute is based in Rio de Janeiro, with branches in Brasília and São Paulo. Igarapé features partnerships and projects in Brazil, Colombia, Haiti, Mexico, Guatemala, the United States and across Sub-Saharan Africa and Western Europe. The Institute receives support from, among others, International Development Research Centre: IDRC, SecDev Foundation, Norway, United Kingdom, the Bernard van Leer Foundation, the Open Society Foundation, the International Development Research Centre, the United Nations and private donors.

Instituto Igarapé
Rua Conde de Irajá, 370 – 3º andar,
Botafogo, Rio de Janeiro – RJ – Brasil - 22271-020
Tel/Fax: +55 (21) 3496-2114

facebook.com/institutoigarape
twitter.com/institutoigarape
www.igarape.org.br

Communications: Alice Watson
Layout: Raphael Durão - Storm Design