The Case of Brazil Reloaded: Interconnectivity and Customization as Key Variables for Cyber Security

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

and

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

NCDG Policy Working Paper No. 14-XXX
Submitted April 24, 2013
The Case of Brazil Reloaded: Interconnectivity and Customization as Key Variables for Cyber Security (*)

Diego Rafael Canabarro 
Thiago Borne

Abstract: Previous work by the authors demonstrated that theoretical controversies in the field of cybersecurity are translated into policy-making without proper empirical grounds. A preliminary assessment of the Brazilian case was presented at the ISA Annual Conference in 2013 (Canabarro and Borne, 2013). The peer reviews conducted at and after the conference (Canabarro, Borne and Cepik, 2013) pointed out to the relevance of information systems' interconnectivity and customization as key-variables for assessing a country's cyber insecurity. In order to support such claim, this paper presents preliminary findings of the evaluation of the Brazilian Federal Police (PF) internetwork. Firstly, it enumerates technical parameters that guide the assurance of critical information systems. Secondly, it presents PF’s mandate and details its spatial distribution over the territory of Brazil. Thirdly, it describes the internetwork solution adopted to interconnect PF’s units. Finally, the paper assesses the complexity of the binominal relation between interconnectivity and customization of IT systems. It then presents the next steps of the research and proposes a framework for comparative analyses with a larger “n”.

Introduction

Research on cybersecurity has focused on the analysis of major events (Estonia, Stuxnet, Wikileaks, etc.) (Mazanec 2013; Nouri 2013; Russel 2013). While important, these events do not represent the majority of cyber-issues usually faced by States (Deibert 2013). These tend to be related to criminal activities, data theft and intelligence gathering instead of full-scale military operations (Rid 2012; Valeriano and Maness 2012; Gendlin 2013). The emphasis on “cyber warfare” has overshadowed the importance of less severe (but not less important) threats and vulnerabilities and the necessity of treating them as a matter of capacity building. The intention of this paper is not to ease the meaning and role of ‘hard’ international security issues and major cyber-events nor the efforts to build macro analytical frameworks for their comprehension, but to show the relevance of a bread-and-butter empirically based approach to cyber capabilities. Such study requires both technical knowledge and access to official and sometimes confidential information.

Therefore this paper furthers the effort carried out between 2012 and 2013 (Canabarro and Borne 2013; Canabarro, Borne and Cepik 2013) to map the Brazilian cyberspace by focusing specifically on the study of critical infrastructure. The paper draws on the parameters set by the “The US-CCU Cyber-Security Check List”, which is a solid framework for the evaluation of the security of critical information systems infrastructure.

It presents a preliminary assessment of the Federal Police (Polícia Federal – PF) computer networks and infrastructure based on the Public e-Procurement Notice (Brazil, 2013a) that established the

(*) Paper presented at the 55th ISA Annual Conference, March 27, 2013 – Toronto, Canada. The authors are greatly indebted to Marcelo Leal, Lidia Lage, and Raquel Rocha, who kindly reviewed and offered insightful comments to the first draft of this paper.

1PhD candidate in Political Science at UFRGS and research assistant at CEGOV/UFRGS.
2PhD candidate in Strategic Studies at UFRGS and research assistant at CEGOV/UFRGS.
characteristics and specifications of the Wide Area Network (WAN) supposed to interlink different internal networks that serve the PF – as well as connecting them to the general Internet – through the employment of the Internet Protocol (IP). In the end, the paper provides some reflections on the binominal relation between interconnectivity and customization of IT systems, contrasting the empirical reality and the necessity of determining the myriad of vulnerabilities inherent to those systems. The paper also presents the next steps of the research and proposes a framework for comparative analyses with a larger “n”.

The research benefited from data collected and organized through a partnership between the Center for International Studies on Government at the Federal University of Rio Grande do Sul (CEGOV/UFRGS) and the Brazilian Ministry of Planning, Budget and Management (MP). The databank provided statistics on the geographical distribution of police units and officials in Brazil. Also, some informal rounds of interview with officials were conducted to settle ground to the study and provide the empirical elements necessary to kick-off the research.

A Roadmap for Cyber Security Research

In order to thoroughly evaluate the Brazilian case, the research employs “The US-CCU Cyber-Security Check List” (US-CCU 2007) developed by the US Cyber Consequences Unit (US-CCU). The US-CCU is an independent research institute established to assess the strategic and economic consequences of possible cyber-attacks and cyber-assisted physical attacks.

The Check List is described in terms of a “risk triangle”, where the three corners are threats, vulnerabilities and consequences (Figure 1). The model employs some basic concepts from risk management and therefore shares the issues usually found in the field. The issues basically relate to the difficulties of defining and measuring each variable and the costs involved in such task (Lowder 2010). The Checklist thus deals only with vulnerabilities, even though it recognizes that its cost-effective appliance requires the accountancy of all three corners of the triangle. “This means understanding the threats enough to have some idea of what kinds of attacks to expect over a given period of time. Even more important, it means understanding the consequences enough to know how critical the various software applications are, how sensitive the various kinds of information are, and what sort of security expenditures are justifiable to protect each of these” (US-CCU 2007, 7).
The Check List is intended as a comprehensive survey of the steps that organizations should take to reduce their vulnerability to such attacks. It encompasses vulnerabilities and counter-measures sorted according to six categories of information system components: (1) hardware, (2) software, (3) networks, (4) automation, (5) humans, and (6) suppliers. Each main area has been subdivided further into two or more “attack avenues” organized according to “the activities that need to be carried out or overseen in order to maintain the security of those information system components” (US-CCU 2007,4). Following this division, an overview of major cyber-attack avenues is comprised of sixteen points: (1.1) physical equipment; (1.2) physical environment; (1.3) physical by-products; (2.4) identity authentication; (2.5) application privileges; (2.6) input validation; (2.7) appropriate behavior patterns; (3.8) permanent network connections; (3.9) intermittent network connections; (3.10) network maintenance; (4.11) remote sensors and control systems; (4.12) backup procedures; (5.13) human maintenance of security procedures; (5.14) intentional actions threatsng security; (6.15) internal policies for software development; (6.16) policies for dealing with external vendors.

The application of such framework for the case presented below, involves a 5-step research program to fully assess the variable characteristics of those sixteen attack avenues. This paper presents the first step: the acquisition of information on the network topology, on the geographical distribution of its nodes and on the function of each node within the network. The other four steps are detailed in the end of the text.

---

The Case: The Federal Police in Brazil

The Brazilian Federal Constitution (Brazil 2010, Chapter III, Article 144) establishes five law enforcement institutions: the Federal Police, the Federal Highway Police, the Federal Railway Police, the Military Police, the Fire Brigade, and the Civil Police, the last three being state police forces.

The PF is the federal investigation police agency of Brazil. It is subordinated to the Ministry of Justice and constitutionally established as a permanent body headquartered in Brasília, with regional offices and a myriad of different agencies in every state (police stations, airports, seaports, outposts, etc.). The PF is assigned by the Federal Constitution to “investigate criminal offenses against the political and the social order or to the detriment of property, services and interests of the union and of its autonomous government entities and public companies, as well as other offenses with interstate or international effects and requiring uniform repression as the law shall establish; prevent and repress the illegal traffic of narcotics and like drugs, as well as smuggling, without prejudice to action by the treasury authorities and other government agencies in their respective areas of competence; exercise the functions of maritime, airport and border police; to exercise, exclusively, the functions of criminal police of the union” (Brazil 2010, Chapter III, Article 144, Paragraph I). It counts among its ranks with approximately 13,836 public officials according to data collected by CEGOV/UFRGS (2013), including agents (agentes), commissioners (delegados), notary agents (escrivães), forensic specialists (peritos), and fingerprint specialists (papilocopistas).

The Agency has broad administrative and judicial powers. Its duties are defined not only by the Constitution, but also by diffuse infraconstitutional legislation. Other federal statutes give the PF the authority to combat terrorism, cybercrime, international drug trafficking, misuse of public resources, organized crime, etc. It is also responsible for tracking and managing the National Weapons System (Sistema Nacional de Armas – SINARM) and firearms borne by civilians, regulating and controlling private security, deploying and maintaining the Civil Identity Register (Registro de Identidade Civil – RIC), issuing passports, establishing and maintaining a database of genetic profiles of criminals, controlling and monitoring chemicals of controlled nature, etc.

The Challenge: Connecting Different Nodes and Systems

PF has over 300 points of presence over twenty-six states and the Federal District of Brazil. In addition to the Central Units located in Brasilia, its regional offices in Brazil are divided in three categories: Regional Inspectorates (Superintendências Regionais), located in each state capital city and in the Federal District; police stations (delegacias), located in non-capital cities; and outposts (postos avançados), spread around the country without formal staffs.
The map below (Figure 2) presents the units located in the territory of Brazil.\(^4\)

**Figure 2 – PF Units in Brazil [Provisional]**

Source: dpf.gov.br and Brasil (2013a).

---

\(^4\) The map was built by crossing information available on the PF Website and on the Public e-Procurement Notice. The map does not show sixty (60) spots for which the information publicly available is either wrong or missing. It does not show the geographic location of facilities that integrate the Tetrapol network (see more below). At the time of writing, there was no information available on the physical location of the new nodes to be created on the network throughout the contract’s term. The map has been constantly updated since the beginning of this research and is available on: [https://mapsengine.google.com/map/edit?mid=zYGKPsbCgLlY.kMQUTdTRmRYE](https://mapsengine.google.com/map/edit?mid=zYGKPsbCgLlY.kMQUTdTRmRYE).
The next map (Figure 3) displays the sixteen Attachés and ten Liaison Offices the PF runs in different countries. According to publicly available information, PF is currently present in Argentina, Bolivia, Canada, Colombia, France, French Guiana, Guiana, Italy, Mexico, Paraguay, Peru, Portugal, South Africa, Spain, Suriname, United Kingdom, United States, Uruguay and Venezuela.

Figure 3 – PF Units in the World

Source: dpf.gov.br and Brasil (2013a).

As of 2012, the PF workforce is comprised of 13,836 public officials (contractors not included). Roughly speaking, this translates to one PF officer for every group of 13,785 people, or one PF officer per 615,5 km². A complete table of the spatial and demographic distribution of PF is presented in Annex 1.

Connecting all these units, both in Brazil and abroad, is a daunting challenge. One has to first consider the geographical factor: Brazil is a continental country, with notable regional discrepancies in terms of infrastructure. In order to connect all PF units, the full use of cyberspace (through radio, telephone, fiber optics, and satellites networks) is necessary as such discrepancies hinder the reliance on a single information and communication technology solution. Security challenges also vary in each part of the country. While big cities like São Paulo and Rio de Janeiro struggle with organized crime and drug trafficking, the western and northern borders usually face problems associated with illegal immigration and smuggling. Furthermore, the PF also has an important social role in underdeveloped regions, where it is responsible for developing public campaigns for disarmament, against child pornography and hate crimes, against people trafficking, etc. Finally, the Policia Federal also runs several Web-based
professional qualification courses for its own staff and broader community, which require the maintenance of three different distance learning platforms, according to the National Police Academy (Academia Nacional de Polícia) Website. It all means that due to its large geographical reach, its overarching mandate, and the sensitivity of its operations for Brazil’s national security, PF requires a very complex and interoperable networking solution for integrating both critical and non-critical information systems. As a matter of fact, expanding the dependence of sensitive networks to a large array of connectivity roads – no matter how customized and exclusive the employed solutions are – magnifies the risks and poses the challenge of dealing with the vulnerabilities inherent to interconnectivity of telecommunication and IT systems (Libicki 2012; Ward 2013).

The Internetworking Solution adopted by PF

In July 2013 – in the middle of Edward Snowden's revelations about American digital espionage in Brazil – the PF launched a Public e-Procurement Notice for IT services. Basically, the e-Procurement Notice aimed at “hiring a company for the provision of telecom services through multiservice IP (Internet Protocol) network using MPLS (Multi Protocol Label Switching) technology to meet the needs of all Federal Police units, providing them solutions for data, voice and images traffic, including the provision, installation and maintenance of circuits and equipment comprising a WAN (Wide Area Network) with proactive management” (Brazil, 2013a).

At the beginning of the 30-month contract, the MPLS network operator is supposed to supply connectivity at the estimated global cost of US$ 41,699,363.71 (R$ 100,612,281.44) for 399 physical nodes all over the country and to interlink that intranet to the global Internet.⁵ They comprise both the 304 points of presence on DPFNet (PF’s computer intranetwork) and the 95 sites where the infrastructure of the TETRAPOL Network (the 470 MHz digital radio communication network employed by the PF) is allocated.⁶ It is expected that by the end of the term, the PF network will be comprised of 682 nodes of DPFNet and TETRAPOL (at cost of US$ 127,718,533.40 or R$ 308,159,450.94). The contract can be renewed for thirty more months.

The contracted company (Empresa Brasileira de Telecomunicações – Embratel) is in charge of providing a full-scale solution for the installation, operation, management, configuration, security, monitoring and evaluation of the MPLS network. Embratel is headquartered in Rio de Janeiro and it is owned by Mexico’s telecommunications giant América Móvil, which acquired it in 2003. The company is a major player in voice and data communication in Brazil, operating fully digitalized microwave communications and fiber optic networks as well as five domestic communications satellites.

The internetworking solution provided by Embratel is supposed to be logically isolated from the Internet, i.e., it has to function as a virtual private network (VPN). In general terms, a VPN counts on proper encryption tools for content and exclusive schemes for addressing, routing and encrypting data

⁵ According to the Project each node of the network currently covers around 21,342 km² and serves a population of 478,051 people and 34 PF officials. By the end of the contract, it is expected that those figures are reduced to respectively 12,486 km², 279,681 and 20.

⁶ The TETRAPOL network was set up by the European Aeronautic Defense and Space Company (EADS) and was designed to provide real-time access to criminal records, geolocation of vehicles and officers through GPS signals and communication channels among those units.
packets (with full interoperability with Internet’s transmission and addressing mechanisms) within its boundaries. In the edges (the ISP Internet Exchange Points), the operators retain full control of what comes in and out the network through traffic management techniques, the use of firewalls, etc. Figure 4 bellow illustrates such architecture in a simplified manner.

Figure 4 – Simplified PF MPLS/WAN Network Scheme

Source: Adapted from 21C MPLS Networks (2014).

Different VoIP and ToIP systems, IT systems and the TETRAPOL network will be integrated through a complex set of backbone infrastructure provided by the contracted company. All nodes in the network will be interconnected through a common and unique group of logical alphanumerical identifiers and protocols that enable end-to-end communication within the PF independent internetwork. In specific Internet Exchange Points owned by the contracted company, that independent network is linked to the open Internet through computers and routers that work as translators of the PF network language to the
Internet language (Internet Protocol [IP] and Border Gateway Protocol [BGP]) and vice-versa. In physical terms, the links between PF sites to the backbone provided by the contracted company and from that backbone to the backbone of ISPs that work as the core of the open Internet are not necessarily dedicated, and are mounted over non-exclusive fiber optics, copper lines, radio signals, and (with some restrictions seen below) even satellites communication.

There are two different sorts of nodes within the network: main nodes and regional nodes. They are distinguished by their mandate and by the characteristics of their point of presence on the network (in terms of equipment specificities, levels and classes of services enabled by the network).

The 32 main nodes of the network are displayed in the image below:

**Figure 5 – PF’s WAN Main Nodes**

They are: the Central IT Coordination Office (inside PF’s main office) and the National Police Academy, both in Brasília; the PF office in “Casa da Moeda”, the state-owned company located in Rio de Janeiro in charge of printing banknotes and manufacturing coins for the Brazilian currency system, as well as other security printings for public and private purposes; the PF offices at the two biggest
international airports in Brazil (Galeão, in Rio de Janeiro; and Guarulhos, in São Paulo); and PF Regional Inspectorates, located in each one of the 26 states and the Federal District. The regional nodes were already depicted in Figure 2. They are all the police stations, airports, seaports, outposts and sites that hold the facilities and equipment of the TETRAPOL network.

The terms of reference for PF MPLS/WAN defined thirty different levels of service, which range from the minimum bandwidth of 512 Kbps to the maximum of 448 Mbps. Most of the levels of service have to count on redundant paths linking the MPLS backbone and the node local router. Levels #1 (512 Kbps) to #10 (8 Mbps, no redundancy) do not specify the nature of the physical link between the node and the MPLS backbone. For levels #12 (10 Mbps, no redundancy) and #30 (448 Mbps), the project specifies the use of either fiber optic cables (for all levels) or digital radio waves (for the majority of them). Level #11 (8 Mbps, with redundancy) occupies the borderline between the two categories: it can operate over fiber optics cables, copper wires, analog or digital radio waves. A specific level of service for the link connecting each node to the MPLS cloud is expressly defined. The central nodes are obviously served by the largest amount of bandwidth. And only the Central IT Coordination Office in Brasilia is to be served the by a level of service #29 in the present and by a level of service #30 by the end of the 30-month term.

The network can support seven different classes of services (five of which demand traffic discrimination and additional efforts for bandwidth management): real-time voice over IP and real-time video over IP (which are delay- and jitter-sensitive); data priority 1; data priority 2; data priority 3; data no-priority; and best-effort. But only the links that serve the central nodes can handle real-time video transmission.

The terms of reference for PF MPLS/WAN expressly specify some contingency and resilience requirements for the two categories of nodes. As a rule of thumb for the project, wherever there is a link with redundancy foreseen, two different and independent access points shall be provided (with a minimum distance of 5 meters between them).

Every main node has to count at least on a router that enables two independent links to the MPLS backbone (one of them to be necessarily built over fiber optics lines). Specifically, the Central IT Coordination Office in Brasilia, and the Regional Inspectorates in São Paulo and Rio de Janeiro have to count on two independent local routers, one for each link to the MPLS backbone, in which they have to be connected to different border routers as well. All of those routers should operate traffic balance for controlling eventual overload. Five seconds is the response-window for the diversion of traffic from a compromised link. As for the regional sites, the connectivity solution for integrating each node to the MPLS backbone is at the discretion of Embratel. The transmission lines can be built, for instance, over technologies such as ATM, frame relay, metro-ethernet, radio waves, etc. Satellite connections can only be employed where it is impossible to rely on terrestrial connections, and the terrestrial hubs for the satellite network have to be located within the territory of Brazil.

The security of the whole MPLS/WAN system is under the responsibility of the contracted company: it is responsible for the physical and logic operation of the network; it has to logically isolate the intranetwork from the open Internet both through addressing/routing and to cryptography/authentication policies, as well as to keep a jealous watch over the border between the two, controlling what comes in and out of the closed network. Logs have to be generated for every event within the MPLS/WAN network. Embratel has the obligation of keeping its equipment (within the perimeter of the MPLS/WAN and its adjacencies outside) updated and properly patched. And,
finally, it has to conduct vulnerability assessments (with no pre-established specific framework) and report the overall scenario every thirty days.

Besides some general specificity regarding the network (its topology and its governance, as well as the reliance by PF on a sole provider) the project does not delve into details regarding the embedded hardware and the software. It only points out to some best practices recognized by the ICT market. There is no detail related to the hardware and software attached to the network’s end. And there are no details of the human factor of the operation of those assets. As a consequence, a much more deep investigation has to be conducted before one can properly jump into conclusions regarding its more or less vulnerability to cyber threats.

**Furthering the Collection of Data**

Once the first phase is concluded, an in-depth evaluation of hardware and software equipment employed within the network and on the edges between the network and the outer-cyberspace is necessary. Accordingly, the governance of the network itself, of its relations with connectivity providers, as well as the characteristics of the IT ecosystem (including the presence in and interconnections with cyberspace) of those providers must be scrutinized.

In the third phase, a round of interviews can be organized both to clarify and complement data raised on the aforementioned phases, and to try to determine the more or less acquaintance of the personnel in charge of the whole interconnected system with the general guidelines of assurance frameworks, such as the US-CCU one. In the present case, the Check List has already been freely translated to Portuguese and selected questions have been forwarded to PF officers through an online form. The questions were selected based on their relevance to the objectives listed by the 2013 Public Notice on TI services. The answers will be processed and compared to the requirements established by the Notice.

In the fourth place, debrief sessions can put closely together public officials and researchers from different fields (Computer and Information Sciences, Social Sciences, Management, Engineering) to reflect upon the findings, to develop appropriate policy responses and to monitor mechanisms. A fifth phase foreseen is the replication of that case study to other governmental agencies as a necessary step for building a comprehensive map that can be employed for risk assessment, either by the Public Administration as a whole or by individual public agencies within the limits of their organization.

**Final Remarks: Empirical Investigation as a Painful (but Necessary) Task**

In November 2013 – only a few months after the e-Procurement Notice release – President Dilma Roussef issued the so-called “Snowden Decree” (Brazil 2013b). The Decree establishes that data communications of the Federal Government shall be conducted by telecom networks and IT services provided by agencies or entities of the federal public administration, including public companies and public-private joint stock companies of the Union or their subsidiaries. The Decree also provided these companies the exemption from the formalities of Procurement Law in Brazil as a way of accelerating the adoption of solutions that enhance national security and the security of critical infrastructure in Brazil. According to the Decree, the Ministries of Defense, Planning and Communications shall
establish joint procedures and deadlines for its implementation, considering each Ministry own peculiarities. The document can be seen as a step towards the strengthening of critical security networks and infrastructure in Brazil after Snowden’s revelations, and was preceded by a series of debates and investigations involving different levels of the Public Administration, including the PF.

For the next thirty months (with the possibility of renewal for thirty more months), nonetheless, the solution adopted by PF will endeavor as a matter of *pacta sunt servanda*.

This paper comprises only the first (out of five) phases of a broader research program to be developed in the future. The difficulties involved at first phase reveal the complexities involved in any empirical research related to cyberspace. Endeavors as such must deal with the multilayered architecture of cyberspace. For every layer (hard and soft infrastructure, logical protocols, applications, users, and governance) there are plenty of available technical and organizational alternatives that can be developed and enacted, either in-house or outsourced. Each of those alternatives results in more or less openness, interconnectivity and interoperability between and among IT systems. It means one cannot take for granted neither full customization nor unrestricted integration and interoperability. The preliminary assessment of the PF case shows that the internetworking solution adopted in 2013 is only partially customized. Despite some minor requirements related to the logic isolation of the MPLS/WAN and to its topology, there is a great margin of discretion to the connectivity provider (Embratel) to take technical decisions regarding the physical integration of each node of the PF network and the technical management of the network, as well as its integration to the open Internet in respect to equipment, software and connecting links. As a matter of convenience, a large portion of the MPLS/WAN is mounted over off-the-shelf solutions.

At this point, it is not possible to detail the characteristics of the network operation that falls within the margin of discretion of the hired company, which highlights the importance of the second and the third phases foreseen for this research to pave the way for the completion of the analysis. Moreover, one has to bear in mind the fact that PF’s network integrates the Brazilian critical infrastructure. It means that part of the information needed for the furtherance of the research is probably classified for reasons of national security. The continuation of this research poses three challenges that are crucial for the quality of research on cyber security.

The first one is to use “access to information” laws in place in Brazil, which may grant us access to non-classified information that is not publicly available yet (which can contribute to public transparency and accountability of the Public Administration in Brazil). The second opens track for the collaboration between academia and the public sector. Solid and responsible research can build a bridge between the policy-making and policy-evaluation arenas. The third challenge reveals a normative horizon related to much of what has been produced in the research field in the last twenty years: the advance of empirical evidence gathering (including evidence that indicates inaccessible information) is a necessary task in order to qualify inferences and generalizations that have been spread, as well as avoid taking mistaken and ungrounded forecasts of “cyber havoc” for granted.

References


GENDLIN, Gerry (2013). “Just War and Cyberwar” (paper presented at the annual meeting of the Midwest Political Science Association, Chicago, IL, April 12, 2013).


