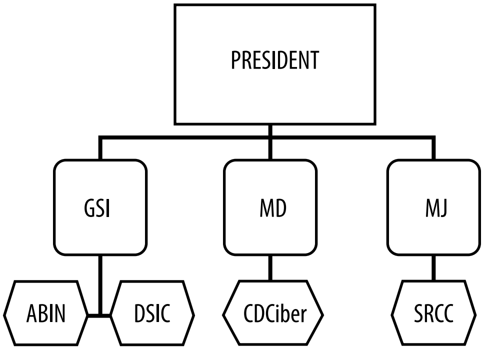
CYBER ATTACKS: IS BRAZIL PREPARED?

Major Luis Eduardo Pombo Celles Cordeiro, Brazilian Air Force

The importance of the cybernetic sector was labeled officially as a “matter of high politics”—related to the survival of the state itself. This statement was made by the Brazilian government in 2008 in a new version of the Estratégia Nacional de Defesa (END) or National Defense Strategy, defining the cyber as one of the three top national security strategic areas along with the nuclear and space.[1] The Brazilian federal government has lain responsibilities of the cyber defense with three principal actors.

- The Gabinete de Segurança Institucional (GSI) or Institutional Security Cabinet with its
    - the Agencia Brasileira de Inteligencia (ABIN) or Brazilian Intelligence Agency and
    - the Departamento de Segurança de Informações e Comunicações (DSIC) or Department of Information and Communications Security,
- the Ministerio da Defesa (MD) or Ministry of Defense, with its:
    - Centro de Defesa Cibernetico (CDCiber) or Cyber Defense Center, and
- the Ministerio da Justiça (MJ) or Ministry of Justice with its
    - Serviço de Repressão a Crimes Ciberneticos (SRCC) or Cyber Crimes Repression Center (figure following)[2]



Brazilian executive branch cyber defense

In the last four years Brazil has hosted six major events:

- the Rio + 20 Summit in 2012,
- the Confederations Cup in 2013,
- the World Youth Day in 2013,
- the World Soccer Cup in 2014, and
- the Olympic and Paralympic Summer Games in 2016.

No major cyber incident was reported at these events proving that, at least on the technical level, the preparation of the Brazil's cyber defenses was effective.

This article will examine the effectiveness of management applied to the cybernetic sector within the Brazilian federal government to answer the question: "Once the state security policy for the cyber-sector has been defined, is it feasible for everyone involved (GSI, MJ, MD) can act in a decentralized way while under a central supervision?"

First, the importance of the cybernetic sector as a matter of high politics, and its relations with Brazilian national defense is examined. Then state actors and their responsibilities are presented with an analysis of the need for centralized management and decentralized execution. A management solution is presented followed by the final conclusions. In the end, this paper intends to show a way to improve Brazilian state's defense capabilities using a strategic management tool in the cybernetic sector—which is indispensable for the contemporary Brazilian society.

The Cyber Sector and National Defense

According to Nazli Choucri, professor of political science at Massachusetts Institute of Technology, the importance of the private sector as a catalyzing power agent is unprecedented. Up to now, the state has been viewed as the only legitimate representative of the national interests in the international relations. Maybe this relationship between state and national interests ought to be rethought to take into consideration the private sector's relevance, particularly regarding cybernetics. It is also important to consider how individual people, using personal resources, can communicate with many persons in a short span of time, increasing their power to influence and simultaneously to be subject to influence. Never before in the history of human relations have individuals gained so much power.[3]

For Brazil, the importance of the cyber sector is explicit in the END, as it considers the cybernetic sector as one of the three strategic areas of defense. The strategic importance of cyber security is particularly the case for the *Força Aérea Brasileira* or the Brazilian Air Force that has to be able to network not only internally, but also with the other Brazilian armed forces in joint operations as laid down in the END. Cybernetic matters have moved from low politics, the state's everyday functioning, to the high politics, the state's survival, as defined in the END.[4]

However from a technological point of view, currently it is impossible for the state to take on the totality of cyber security responsibilities because neither the private sector nor citizens are willing to surrender their cyber power and delegate it to the State. Two recent developments illustrate this. Brazilian judges, on more than one occasion, have banned the Whatsapp application claiming that the software developer was not passing on the requested data in response to court orders. In all these instances, Brazilians simply migrated to similar applications such as Viber and Telegram. Then the individual judges were attacked with accusations of megalomania, lack of empathy, functional incapacity, and so on. Ultimately the entire Brazilian judicial system came under public censure, and no Whatsapp ban lasted more than 48 hours before being revoked in by higher courts.[5]

In 2016, before the parliamentary *Comissão sobre Delitos Cibernéticos* or Commission on Cyber Crimes, the head of the SRCC, agent Elmer Vicente Coelho, was emphatic in stating that many of the companies that operate in the software market, such as Whatsapp, do not have subsidiaries or representatives in Brazil and they simply ignore Brazilian law. The Brazilian state apparently has no power over what the company does, even though it is one of the most popular communication softwares in the country.[6] In cases such as this, the state must act with caution to not exceed its power over the private corporations and citizens and move toward totalitarianism. The solution to the problem should focus on the cyber sector's systemic organization rather than the operational or tactical "state of the art" since that expertise (operational and tactical) lies in the private sector.

According to Professor Walfredo Bento Ferreira Neto, the United States of America (USA) has six federal agencies focusing on national and international network defense, and it is the National Security Council that defines the state's policy for this sector and the occupation of each agency. For example, defending military networks' infrastructure and extraterritorial actions is US Cyber Command's responsibility, and the security of the national civil infrastructure is the responsibility of the Department of Homeland Security.[7]

The Ferreira Neto also provides examples of countries that followed the USA's model and started to organize themselves to defend their interests in the virtual environment:

- the Office of Cyber Security for the United Kingdom,
- Cyber Security Canada,
- the Cyber Security Strategy for Germany, and
- France's Défense et Sécurité des Systémes d'nformation: stratégie de la France,
- and specific entities for this sector in China and North Korea.[8]

Brazil has also followed similar lines of reasoning.

The Main Actors in Cybersecurity Defense

A study by Raphael Mandarino Jr. of the Federal University of Minas Gerais showed that there were sixteen organizations spread between ministries and secretaries and federal authorities responsible for assisting and protecting against cyber threats in 2010. That makes it necessary to highlight a few considerations:[9]

1. None of these organizations have hierarchy or administrative jurisdiction over the others since each one of them operates in a specific field of public administration. For example, the GSI determines the information technology policies for the whole of the federal go-

vernment. However, it cannot determine where the operational fields of the CDCiber or the SRCC of the Brazilian Federal Police begin or end because these agencies are subordinate to different ministries. In reality, each agency looks out for their necessities. This is understandable, and therefore there is no "boss" or "czar" managing all these efforts from a single strategic point of view.[10]

2. When discussing technology the private sector cannot be excluded from the discussion. This is because the cyberspace accessibility at the individual level is possible because of artificial environments that were created and maintained by people. Nowadays, this power to create and sustain has devolved to the private technology sector.[11]
3. The rest of the private sector are not the masters of these technologies but are completely dependent on the technologies. Banks, energy, mining, and food companies, and current industrial activities are dependent on technological development to be able to thrive in the current market. So, whoever has the power over this technological development also has the influence on the state's most important economic agents and consequently on the state itself.[12]
4. It is highlighted that this influence is even stronger over the essence of a nation: the individual citizen. Citizens cannot give up communicating through a cell phone or managing their life using a personal computer and software.

Together with the four state actors mentioned before (ABIN, DSIC, CDCiber, and SRCC), we also have the private sector and the citizens. All of them are involved in cyberspace, and each has specific needs. On the other hand, with the importance of cyberspace for the security of society requires the state to protect it.

The actors in the cybernetic security sector have been identified. It is concluded empirically that those actor's objectives are diverse and that it is the responsibility of the state to ensure security in cyberspace. It can be affirmed that the role of the Brazilian government should be that of coordinator—performing centralized management which allows a decentralized implementation of cyber security.

The launching in 2010 of the *Livro Verde de Defesa Cibernética—The Green Book of Cybernetic Defense*—can be considered an initiative in building a collection on cyber security efforts. The GSI tried, for the first time, to establish some potential strategic guidelines for the cyber sector. However, the complexity of managing so many interests can be one of the reasons why, up until today, there isn't a *livro branco de defesa cibernética*—a white book of cybernetic defense, in which the national cyber security policy would be clearly defined. This condition also exists because of the wide gulf between the government and the society on the subject.[13]

However, for the sake of discussion, assume that this white book has been released and Brazil does have a "national policy for cybernetic defense." With the premise that it would not be appropriate for just one actor to be responsible for the management of the whole policy. An hypothesis is formed: "The adoption of a strategic management tool will increase the national ability to reach the national objectives." The "national cyber office" should be designed in a holistic way to implement the national policy for cybernetic defense to allow an integrated vision representing all the actors across the cybernetic sector. Without this strategic view of cyber security, a discussion about a comprehensive and interdisciplinary approach to the problem is difficult. Members of the technology sector will worry more about their necessities, the members of the private sector will be directed by their separate objectives, and the state—representing Brazilian national security and the security of individual citizens—will be directed by the distinct perspectives of its agencies, the ABIN, the DSIC, the CDCiber, and the SRCC.How would it be possible to coordinate all these interests and at the same time not interfere with them?

A solution to this dilemma may be the adoption of Harvard Business School's Robert S. Kaplan and David P. Norton's concept of strategic management (SM) and the creating of an *uni-*

dade de gestão estratégica (UGE) or office of strategic management, to take into consideration the interests of all of the stakeholders involved and increase the ability to reach the intended goals.12 This proposal is based on the concept described by Kaplan and Norton the UGE would operate like "the engineer of a sophisticated watch keeps all mechanisms in sync despite them rotating in different velocities." The UGE could be capable of retaining the individuality of stakeholders and supervise how each one of them acts in accordance with a national policy without direct interference in their individualities.[15]

At least three issues are raised, however, in the use of the UGE as a tool to implement the national policy for cybernetic defense:

- the numbers of people required to implement and manage the process,
- the UGE does not seem appropriate to coordinate with state agencies because its underlying concept was developed for civilian corporations with the aim to generate profits, and
- the stakeholders and their interests are dispersed inside and outside the government making it impractical to develop solutions that fit in all cases.

The SM concept was successfully used by the Chrysler Group where they managed to put 13 people in charge of a "strategy scorecard" program encompassing related material to more than 90,000 employees by 2000. In fact, a UGE has nine divisions that, within the concept adopted, could theoretically be managed by only nine people.[16] Extrapolating from the Chrysler example to the Brazilian reality, we see that the total active personnel of the cyber security agencies—ABIN, DSIC, CDCiber, and SRCC—it is something around 350,000 people. So, disregarding some systemic factors, we can estimate that an office of around 50 people could implement and manage the national cyber defense policy. This team would also be responsible for liaising with tech firms, private companies, and representatives of society—from associations and organizations to individuals—who want to participate in the process.

Obviously, this is only an estimate and probably unreliable without studies being made to confirm it. However, if the objective of the UGE is to verify that policies are being implemented, then the agency's size will depend on the complexity and depth of that process. The personnel requirements will be as large as the task to be performed—there is no problem regarding the numbers of people involved as they will vary according to the decision-maker's will.

In the question of the applicability in the governmental sector, the US Army Balanced Score Card Project was able to develop its UGE in 2005. The military version of the office took on the role of a strategic communication security program that included 13 major commands and more than 300 subordinate commands around the world. This proves that the same principles would apply to both state and private actors.[17]

Both UGEs, Chrysler and the US Army, were seen as "command and control tools," designed to check the results and eliminate local initiative, in practice, exactly the opposite was the result. Local ideas could "be put on the agendas of quarterly and annual strategy reviews, with the best concepts being adopted and embedded in enterprise and business unit strategies."[18] That way, the UGE does not interfere with the intrinsic activities of each member of the system and has the responsibility of integrating the related activities, managing the strategic and operational management processes, and structuring the inclusion of management processes that may be useful. In this way, the UGE can adopt an holistic view of the entire process, pursuing the strategic objectives and, at the same time, allowing for individual interests.

With more transparent communications, all the society will gain. Decision makers at the strategic level will have their policies broadcast, the stakeholders can become active participants in the strategic planning, and the UGE agencies will not only be capable of implement the national policy for cybernetic defense but will also be able to improve it.

CONCLUSION

The capabilities provided by the cyber technology have become a vital asset in the relationship between the government and society. Consequently, actions are being taken to guarantee the protection of the national interests in the cybernetic sector, but it has been proven that this kind action is difficult. The state does not have complete control over the private sector with cyber security issues. Governments have been forced to take indirect actions in the cybernetic field through their agencies instead of directly regulating the cyber sector in due to the complexity of the matter.

This complexity arises out of the multitude of needs, objective, and interests of individual citizens, the technology sector, the private sector, and the several government agencies charged with implementing cyber security. Brazil's defenses are weakened by the lack of centralized cyber security authority that can formulate and implement security strategies and policies. The diversity of interests in the virtual realm seems to make impossible such centralization. As a solution to this dilemma, it was proposed the concept of the UGE as a valid solution.

That way, we understand that the adoption of the UGE will allow the implementation and development of a future national policy for cybernetic defense, and increase the ability of the Brazilian government of reach the national objectives. Once the principle of centralized control and the decentralized execution is implemented through strategic management, Brazil's ability to manage the cyber sector will be improved.

Certainly, this does not close the matter. It stimulates new questions about the importance of the cybernetics within the concept of national power and the role of the GSI as a central agent of a future national policy for cybernetic defense. Preparing to answer these questions, among others, is a challenge for Brazil today.

Notes

[1] Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA: MIT Press, 2012), 227–30.

[2] Ministério da Defesa (Ministry of Defense, Brazil), *Política Nacional de Defesa e Estratégia Nacional de Defesa* (*National Defense Policy and National Defense Strategy*), (Brazilia: 2012), 6, http://www.defesa.gov.br/arquivos/estado_e_defesa/END-PND_Optimized.pdf.

[3] Elmer Coelho Vicente, *Testemunho na Comissão sobre Delitos Cibernéticos* (*Testimony in the Commission on Cyber Crimes*), (Brasília: Câmara dos Deputados [Chamber of Deputies], 28 August 2015). http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar- de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/notas- taquigraficas.

[4] Ibid.

[5] Walfredo Bento Ferreira Neto, *Segurança e Defesa Cibernética: da Fronteira Física aos Muros Virtuais* [*Security and Cyber Defense: From the Physical Frontier to the Virtual Walls*] (Recife, Brazil: Editora UFPE, 2014), 81.

[6] Ibid, 82.

[7] Raphael Mandarino Jr., *Segurança e Defesa do Espaço Cibernético Brasileiro* [*Security and Defense of the Brazilian Cyber Space*] (Recife, Brazil: Cubzac, 2010), 119.

[8] Nival Nunes de Almeida and Eduardo André Araújo de Souza, *Arcabouço Político-Administrativo do Espaço Cibernético Brasileiro* [*Political and Administrative Framework of Brazilian Cyberspace*] (Florianópolis, Santa Catarina State, Brazil: IX Encontro Nacional da Associação Brasileira de Estudos de Defesa [IX National Summit of the Brazilian Association of Defense Studies] 6–8 July 2016), http://www.enabed2016.abedef.org/resources/anais/3/1466280464_ARQUIVO_IX_ENABED_ARCABOUCO_EDUARDO_NIVAL.pdf.

[9] Nazli Choucri, *Cyberpolitics in International Relations* (Cambridge, MA:MIT Press, 2012), 230–233.

[10] Ibid.

[11] Gabinete de Segurança Institucional [Office of Institutional Security], *Livro Verde de Segurança Nacional* [*Green Book on National Security*] (Brasilia: Presidencia da Republica [Presidency of the Republic, Brazil], 2010), 5–15.

[12] Robert S. Kaplan and David P. Norton, "Office of Strategy Management," *Harvard Business Review*, October 2005, https://hbr.org/2005/10/the-office-of-strategy-management.

[13] Robert S. Kaplan and David P. Norton, "Office of Strategy Management: Emerging Roles and Responsibilities," *Harvard Business Review* 10, no. 4 (July–August 2008): 2.

[14] Robert S. Kaplan and David P. Norton, "Office of Strategy Management," *Harvard Business Review*, October 2005, https://hbr.org/2005/10/the-office-of-strategy-management.

[15] Ibid.