THE CYBERNETIC THREAT FOR THE SECURITY AND DEFENSE OF BRAZIL

In the era of Digital Revolution, technology has become a very important factor. However, Internet may be a double- edged sword, as it is sometimes a useful tool and some other times a threat with respect to which institutions controlling security and defense of a nation must be alert. This is why Brazil has decided to implement policies to face a latent cybernetic threat

KEY WORDS: **CYBERWAR / THREAT / SECURITY / VULNERABILITIES**

By **Augusto Cesar Amaral**

Translated by Mariana Ríos Hudson

The 21st century is known as the century of the Digital Revolution because of the progress in computing and telecommunications. As any other tool, technology may be used for the progress of humankind or any other purpose. Nowadays, we cannot say that a country may not suffer a cyber- attack that implies not only a cybercrime but also a state cyber aggression in its different ways.

Thus, cybernetic threat affects security and defense of any state. Brazil is not an exception to this. However, what is the importance of this threat? What are the main vulnerability factors?

Based on the Brazilian National Defense Policy implemented in 2005, we will explain the way in which its capacities for Cybernetic Security and Defense of the National Critical Infrastructure are organized and we will try to answer the following question: Is Brazil able to provide an effective defense against attacks carried out in an increasingly hostile cybernetic scenario?

CONCEPTS AND DEFINITIONS

The great technological progress made during the last 30 years in the field of Information Technology and Communications (ICT) has led to significant changes in the way individuals, organizations and nations relate among each other and are organized.

Nowadays, we can see a great dependence of individuals, social groups, public and private organizations, government critical structures, countries' security and defense on information systems that are interconnected through complex data processing networks. These are vulnerable to attacks and fraud by different agents in a new interaction space called cyberspace:

An environment characterized by the use of electronics and the electromagnetic spectrum to store, modify and exchange data through a network system and the associated physical infrastructure. Cyberspace may be considered an interconnection of human beings through computers and telecommunications without considering its physical dimension[1].

...it includes the organizing structure of the Internet, devices connected to the Internet as well as conventional and wireless networks. Some of these networks are administered by government and private entities, some are connected to a broader Internet and some are not[2].

In essence, security refers to the condition of being secure, free from risks and/or threats, danger and, if necessary, to be able to defend oneself with high probabilities of success. Defense is the action carried out to protect oneself against such risks, threats, danger and damage[3].

We can, thus, state that, within a state, cybernetic security refers to the protection and guarantee of use of information strategic assets that control the national critical infrastructure[4]. Cybernetic defense refers to the setting of defensive or aggressive actions in the context of military planning to be carried out in cyberspace and which may cause a cyberwar.

CYBERNETIC THREATS AND VULNERABILITIES

There is much news about cyber- attacks against citizens, organizations, companies and critical structures of a country. These may come from anywhere and it is very difficult to identify their author or source. They may be launched by young amateurs without great intentions, economic fraud criminal groups, industrial espionage companies, terrorist groups for political purposes or even state agents.

There are many associated risks and systems vulnerabilities. Most acts come from the attraction that cyberspace causes as it offers greater profitability, globalness and ease, impunity for any type of activity.

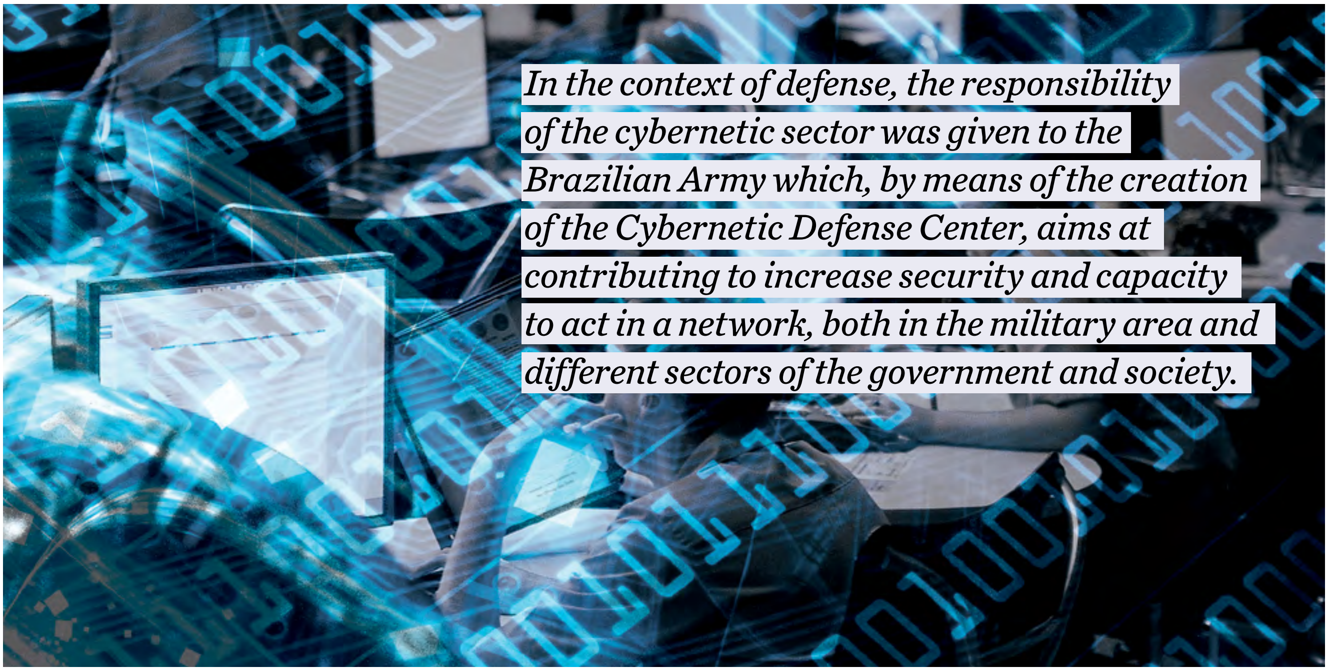
Conflicts may be as simple as civil disputes over the ownership of a domain name or more complex disputes such as deliberate campaigns of cyber- attacks as part of a conventional war among technologically advanced states.

It is important to make a distinction between cyber threats and crimes as most cybercrimes do not even represent a threat for the security of the country because they do not affect their critical infrastructure and they have to be dealt with in the areas of justice and law.

However, some analysts consider that: the feeling of insecurity in the network and the alarming existence of cybercrimes are the result of information resources artificially created by the cybersecurity industry which, of course, is interested in exaggerating cybercrimes; that is, in the creation of a subjective feeling of insecurity and alarm in the network[5].

Others, such as David Betz and Thomas Rid question the use of the term cyberwar saying that:

The term cyberwar is, of course, intriguing. But what does it actually mean for strategists concerned about the



In the context of defense, the responsibility of the cybernetic sector was given to the Brazilian Army which, by means of the creation of the Cybernetic Defense Center, aims at contributing to increase security and capacity to act in a network, both in the military area and different sectors of the government and society.

Cybernetic threats affect security and defense of any state. Brazil is not an exception to that. However, what is the magnitude of this threat? What are the main vulnerability factors?

balance of ends, means in conflicts nowadays? Not so much. In fact, it is not only a neologism of meaning, but it is also a distraction with no sense in strategic terms. Contemporary strategists who consider that cyberwar is a new decisive form of conflict are mistaken[6].

Cyberwar has never happened in the past: this does not happen today and it is unlikely to affect our future. All prior and current political cyber- attacks –as opposed to cybercrimes- are sophisticated versions of three activities that are as old as human conflict: sabotage, espionage and subversion[7].

BRAZIL

In 2005, after a long period of time without a defense policy, the Brazilian Government issued its National Defense Policy –PND[8], in its Spanish acronym, a document that has the purpose of making all sectors of Brazilian society aware of the importance of the country's defense.

It sets forth that the cyber sector is strategic for National Defense which must be strengthened in order to reduce vulnerability of systems that have support for information technology and communication or allow its quick recovery. Therefore, it must be able to oppose to possible cyber-attacks.

Also, when it comes to national security and measures for critical infrastructure security, the National Defense Strategy –END, in its Spanish acronym (2008), mandates the enhancement of devices and security procedures that reduce vulnerability of systems related to National Defense against cyber-attacks and, if necessary, that allow for its quick recovery, under the responsibility of the Chief of Staff of the President of the Republic, the Ministries of Defense, Communications and Science and Technology and the Institutional Security Cabinet of the President of the Republic.

The Institutional Security Cabinet, an entity that coordinates the activity of information security in Brazil, launched in 2010 the Libro Verde de Seguridad Cibernética [Green Book on Cyber Security] with the purpose of creating the necessary conditions for cyber security with respect to the understanding of new requirements for the protection of the Brazilian state and society.

This book aims at facing the challenge of gathering the agendas of the government, schools, the private sector[9] and the third sector in an effort to build common thought and guidelines for a Cybernetic Security National Policy including the following factors: political and strategic, economic, social and environmental, communications and information technology, education, legal affairs, international cooperation and security of critical infrastructure. It considers cyber security a strategic responsibility of the state that is key for the maintenance and preservation of critical infrastructure of the country, such as energy, transport, telecommunications, water, finance, information, among others.

In the context of defense, the responsibility of the cyber sector was given to the Brazilian Army which, through the creation of the Cybernetic Defense Center, aims at

[1] Bejarano, María José Caro; "Alcance y Ámbito de la Seguridad Nacional en el Ciberespacio" [Scope and Context of National Security in Cyberspace]; Cuadernos de Estrategia 149; Cybersecurity. Challenges and threats to national security in cyberspace; Instituto Español de Estudios Estratégicos; Spain Ministry of Defense; 2011; chapter 1; pages 49 – 82.
Available at http://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

[2] Chang, W., & Granger, S.; "La Guerra en el Ámbito Cibernético" [War in the Cybernetic Field]; Air & Space Journal - Spanish, Volume 24, No., 3; pages 83 - 90. Available at http://www.airpower.au.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_10_chang_s.pdf

[3] de Vergara, Evergisto; "Las diferencias conceptuales entre Seguridad y Defensa" [Differences between the concepts of Security and Defense]; Instituto de Estudios Estrategicos de Buenos Aires – IEEBA; febrero de 2009. Rescatado de http://www.ieeba.com.ar/colaboraciones2/Las%20 diferencias.pdf

[4] Critical infrastructure refers to facilities, services, goods and systems, the interruption or destruction of which will cause serious economic, social, political, environmental, international or State and social security impact; Brazil; Institutional Security Office; Livro Verde: segurança cibernética no Brasil; 2010.

[5] González Cussac, José Luis; "Estrategias legales frente a las ciberamenazas" [Legal strategies for cyber threats]; Cuadernos de Estrategia; Nro. 149; Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio [Cybersecurity. Challenges and Threats to national security in cyberspace]; Instituto Español de Estudios Estratégicos; Spain Ministry of Defense; 2011; Chapter II; pages 85 - 127.
Available at http://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf

[6] Betz, D.; "Cyber war is not coming. Infinity Journal"; Issue Nro. 3, Summer; 2001; pages 21 – 24.
Available at https://www.infinityjournal.com/article/23/Cyberwar_is_not_coming/

[7] Rid, T.; The cyber war will not take place. London: C. Hurst & Co.Ltd; 2013.

[8] Decree No. 5484; June 30, 2005; Brazil.
Available at http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm

[9] Third sector usually refers to a group of institutions whose main characteristic is to be "private but not profitable" and to act in the public sector to meet demands that are not met by the State or the market. This is a highly diverse scope of organizations that act within a non- profitable sector (non- governmental organizations, foundations, school canteens, cooperatives, etc.), which authors usually call in different ways: non- profitable sector, social or solidarity economy, third way or third sector.

[10] Portaria Normativa; N° 3389 /MD; Brazil; December 21, 2012. Available at: https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf

Cybernetic defense refers to the implementation of defense and attack ations in the context of military planning to be carried out in cyberspace and which can lead to cyber war.

increasing security and capacity to act in a network both in the military area and in different sectors of the government and society.

The Defense Center focuses its actions on the training of human resources, doctrine updating, security enhancement, response to network incidents, incorporation of lessons learned and protection against cyber- attacks.

Following the ongoing process, the Ministry of Defense published in 2012 a document that explains the Cybernetic Defense Policy[10] and sets forth the guidelines for the Cybernetic Defense Military System (SMDC, in its Spanish acronym) to consolidate itself. The document indicates the responsibility of the Armed Forces in the prevention of the criminal use of the Internet and other networks as well as the protection of date and essential communications.

SECURITY SYSTEM AND CYBERNETIC DEFENSE

Nowadays, we can say that Brazil is about to consolidate the Brazilian Cybernetic Defense Military System. This will be applied at national level and has been prepared at the highest political level, represented by the Institutional Security Cabinet (GSI/PR, in its Spanish acronym) and the Federal Public Administration (APF, in its Spanish acronym), and has been through the Ministry of Defense (MD, in its Spanish acronym) which is in charge of the strategic- political relation and reaches the lowest levels of command of the Armed Forces that act at operational and tactical level with the purpose to involve the whole society in the defense of national interests in cyberspace.

In this system, the Security Cabinet (GSI/PR) coordinates actions that affect security of the society and the State: Cybernetic Security, Communications and Information Security and National Critical Infrastructure Security.

Apart from contributing to the national effort in the areas of security, the Ministry of Defense is responsible for Cybernetic Defense operations.

For this purpose, the Armed Forces have received this command:

- **At strategic level:** to carry out the necessary actions for their performance in situations of crisis or armed conflict and episodic characteristics in a situation of peace and institutional normality.
- **At operational level:** to carry out defensive and attack actions related to the preparation and use in military operations of any nature and intensity that are inherent to cyber- war.

CONCLUSIONS

Can Brazil provide an efficient defense against attacks originated in an increasingly hostile cyber environment?

We can nowadays say that there is no country capable of defending itself against cyber-attacks in an efficient way. Context constantly changes and new threats appear every moment. Data processing and information systems are, in general, very vulnerable and actors involved are very different among them.

It is impossible to predict an attack or identify its origin with precision. Security sectors focus their actions on the identification and elimination of vulnerability points of the systems used and the capacity to recover themselves and not to replicate damage after the attack.

In this sense, Brazil, as some other countries, has the purpose to create awareness and involve the different sectors of the Brazilian society, including the political area, the armed forces, academics, the private sector and the third sector as to the problem of security and cyber defense.

Brazil has worked to organize and train agencies related to security and cyber defense, information and communications security, security of critical infrastructure which develop activities that complement and overlap among them.

It has also designed the Brazilian Cyber Defense and Security System which is coordinated by the Institutional Security Cabinet of the President of the Republic and is supported by the Ministry of Defense as regards defense actions.

There, cyber defense is mainly developed by the Cyber Defense Center of Brazil, a recently created military unit that has the purpose of generating knowledge and doctrine, train human resources and apply defense and attack actions of cyber war.

We can conclude that Brazil has all the necessary conditions to develop its Cyber Defense and Security System and, therefore, face any attack that may affect the functioning of its critical infrastructure.

› REFEREED ARTICLE

Augusto Cesar Amaral
Colonel of the Air Force of Brazil. Staff Officer. He has graduated from the Joint Forces Staff College in 2013 with the Course on Leadership and Joint Military Strategy at the Strategic Level