Brazilian Cyber Power

A New Perspective on the Expression of National Power

Major Luis Eduardo Pombo Celles Cordeiro (FABRA)

Introduction

How important is defense in a country like Brazil, with shortages in several other areas such as health, safety, and education? We've heard this question several times in debates on media programs, in the press, and in scientific articles.

The premise of this question is based on the absence of external and internal "traditional" threats (as defined by international relations theories) that may affect our integrity as a nation. This logic may lead us to the conclusion that defense should not be a priority in the development of our national policies and should be considered a matter of "low politics."

To refute this reasoning, we chose to use the theory of lateral pressure (Choucri, 2012), which says that nations have a natural tendency to extend their influence and/or territory to meet the domestic demands of their population. So to increase its presence, physical or otherwise, beyond its borders, a country will apply "lateral pressure" in another country or countries at the desired position. Thus, we conclude that lateral pressure is part of international relations between states.

Therefore, we can assume that Brazil, like any other country, will exert lateral pressure on the international scene to satisfy its internal demands and will suffer such pressure from other nations.

This article focuses on a particular element of this game that currently affects the core functioning of our society: cyber power. It is first necessary to define cyber power, then to identify its area of influence in our society, and finally to propose ways to develop instruments of cyber power on behalf of our national defense.

Power

Power itself is a very difficult and abstract concept to explain, although many have tried to do so. Galbraith wrote a book about it and concluded that “”Few words are used so frequently with so little seeming need to reflect on their meaning as power, and so it has been for all the ages of man” (John K. Galbraith, “The Anatomy of Power”,1983.

Max Weber, on the other hand,argued many years earlier that the exercise of power by the state is simply the domination of men in a position of authority allowing them to impose their will on their countrymen(Weber, 2001). Looking at relationships among people, Raffestin wrote that wherever there are humans in relationship, there will be a relationship of power because the individuals will have divergent interests (Raffestin, 1993). Therefore, we conclude that the struggle for control and power between two individuals (or groups of individuals) means imposing one’s will on the other, and this is a basic notion in discussing power relations.

National Power

To discuss the state-power parameter in international relations, we use the ideas of the Basic Manual from the Brazilian War College (ESG) because its interdisciplinary view and its focus on national defense, as described in the manual (ESG, 2011), provides an adequate vision of the subject from our perspective.

According to ESG doctrine, the state should try to serve the desires of the nation (the so-called national objectives) through the use of its available resources (the national power) to achieve the objectives set (through a national policy) so that in the end the correct application of national power will allow the nation to achieve its national objectives in accordance with the goals set by its national policy. So the state’s ability to ensure that its stated objectives are met depends directly on the state’s capacity to work both with its international allies and its own population in different environments (economic, cultural, military, social, etc.).

ESG establishes two key concepts: safety, which is the sense a person has (and therefore society as a whole has) that he or she is protected against internal and external threats; and defense, which is the actions that ensure the state’s sense of security. As the manual explains, “In conclusion Security is a feeling, while the Defense is the action” (ESG, 2011).

According to the ESG’s definition, today we have five expressions of national power: political, economic, scientific and technological, psychosocial, and military. These expressions are the instruments used in defense activities to provide the feeling of security to the nation.

The Brazilian Department of Defense affirms that to make the best use of these expressions, it is necessary to know that the relationship between them can vary in space and time according to the groups involved and their interests MD51-M-04, 2007). In particular, in the use of the military expression, this relationship between space and time is a critical factor for the freedom of action of the actors involved and therefore in the state’s ability to enforce its will (MD30-M-01, 2011).

Since the assurance of defense is a product of the correct notion of space and time, it is important that we establish the notion of time (when) and space (where) used in this article and how it relates to cyber power.

Space and Time

One can think about space in many ways. Here we are going to use a concept different from that of classical physics, which says that distance (synonymous with space) is measured in direct relation to the time it takes to cross it. Although we also say that space is related to the time it takes to cross it, we use Harvey's idea of "time-space compression." In his line of reasoning, if in 1840 a letter could travel at a speed of 10 miles per hour, in 1930 its speed would have increased to 65 mph, in 1940 to 400 mph, and in 1960 to 700 miles per hour (Harvey, 1989).

Following this logic, we can conclude that at the present time the same message is moving at the speed of light (limited by the transmission system) via the Internet, an extranet, or an intranet. Based on this reasoning and using as an example a telegram sent from São Paulo to Rio de Janeiro, we see that the distance between the two cities (around 260 miles) has not changed significantly since their foundation in the sixteenth century, but the effects of the same message will be felt more quickly today than ever.

So what we are looking at today is the transformation of space into something ephemeral, where going to your neighbor's a few feet from your front door to ask for a cup of sugar will consume more time than sending and receiving an instant message, a photograph, or a text from a friend in Beijing.

If in the first case we move by foot and in the second via a message on the phone, we may have the answer from our friend in China before our encounter with our neighbor. Accordingly, we conclude that if the sense of space is basically connected to the concept of time, we can say for sure that space is not the same thing as distance when we are talking about communication. While the distance is fixed and based on the measurement used by the observer (meters, feet, miles, etc.), the space in communication depends on the time required for the information to be produced and sent from the transmitter and received and interpreted by the receiver, regardless of the distance.

This rapid communication we see today creates the perception that we have moved from a rigid society, where the communication workflow is restricted and rigid, to a fluid society where information flows between individuals in an atmosphere of anarchy (in the sense of freedom or lack of control), no longer ruled by the distance between the parts involved but by the tools that allow this real-time communication.

This view was proposed by Bauman early in this century, in a concept he calls "liquid modernity." Accoordingly, changes in a society "flow," and society assumes the shape of the environment containing it, whereas society was previously "solid" and required strength and pressure to be molded into a new form (Bauman, 2001). This liquidity in today's world allows changes to penetrate all layers of life, including the space-time relationship. The current rate at which information is exchanged means the individuals communicating no longer have to be physically present. They can be virtually present through technology. A person's "presence" (as well as that of others who are part of the person's social, family, or professional circle) is replaced by software on the computer that creates the virtual person. Since the notion of space-time becomes extremely small, it is not necessary to go somewhere to be "present," or rather, the no longer takes place in the real world but in the virtual world, which is the concept of "space traveled in a given time" currently used for interaction between people today.

We realize, therefore, that the "real" need to move from one place to another in order to interact (and, therefore,to interact in a relation of power) will be replaced—if not completely, at least in part—by the need to stay connected to the virtual world. This need directly influences the notion of past, present, and future in human relations and shrinks our notion of space in a world where the access to information and the ability to communicate increase exponentially.

All of that is because of the evolution of technology (portable or not) and its ability to provide access to communication networks in which an individual can represent his or her desires, opinions, and claims without the need to be tied to a collective representation such as associations, unions, political parties, NGOs, and similar entities (Choucri, 2012).

These information tools allowed us, in the 1990s, to enter what Peter Drucker called the information age. In the information age, activities should focus on the production and dissemination of knowledge to generate wealth (Drucker, 1999).

So we note the importance of these devices that allow us to interact in this modern way, and it is easy to understand why keeping them running is important to a feeling of security, not only for individuals but for the institutions of the Brazilian state.

Therefore, it is necessary to provide the ability to communicate with safety, but without losing the values enshrined in our social contract: freedom of expression, the right to choose your political preferences, the right to own property and assets (either real or virtual), and all other rights granted in our constitution. In other words, it is necessary for the state to exert its national power in this virtual environment. But before the state chooses how to exert this power, it is necessary first to delimit the scope of action, and in our opinion this task calls for the creation of a new expression of national power:cyber power.

Cyber Power

The term cyber power does not exist, at least not in the usage proposed by this author. What we see in the literature with considerable frequency are definitions with an approach focused on action in cyberspace, namely the Internet:

- Cybersecurity Strategy: "The practical art of ensuring the existence and maintenance of the information society in a nation, and guaranteeing and protecting, in cyberspace, their information assets and critical structures" (Mandarin JUNIOR, 2010).
- Cyber War: "The actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption" (Clarke and Knake, 2010).
- Cyber Power: "The ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power" (Daniel T. Kuehl, From Cyberspace to Cyberpower, Chapter 2).
- Cyber War: "A set of actions for offensive and defensive use of information and information to deny, exploit, corrupt or destroy the values of the opponent based on information, information systems and computer network systems" (Ministry of Defense, 2007).
- Cyber Deterrence: "The capacity in cyberspace to do unto others what others may want to do unto us " (Libicki, 2009).

The concept that perhaps comes closest to this proposal may be contained in the military doctrine of joint operations written by the Brazilian Department of Defense, where cyber power is defined as the "ability to use cyberspace to create advantages and influence events in all operating environments and other instruments of power."

But in the same document, when we look for the definition of cyberspace, we find that it only considers the virtual environment where data must be transmitted, processed, or stored (MD30-M-01, 2011). In these definitions, we believe that the scope of the term does not include all the constituent elements of cyber power since the definitions no longer take into account the individual ("humanware") or hardware, key elements, in our opinion, to construct the idea of cyber power.

Thus the concepts currently linked to defense and cyber issues are in a pre-pragmatic phase, according to the structure described by Thomas Kuhn (Kuhn, 1991). This is because there is no consensus on the essence of how the issue should be looked at. Should it be examined through a philosophic, cultural, military, or economic view?

So we find today that the Brazilian state is acting in response to situations that are actually happening and not planning for the future through future-oriented strategic planning. This results in a capillary effort, with each federal entity affected by these new forms of interaction trying to meet its own needs.

As an example of such a division in the structures responsible for providing cyberspace security (according to the concept presented by ESG) in Brazil, Mandarino wrote that in 2010, 16 institutions—scattered among agencies, departments, and bureaus—were responsible for the cybersecurity of the Brazilian executive branch in the federal government (Mandarino, 2010). But at the strategic level, where the objectives defined by Brazilian cybersecurity policy are achieved, and at the tactical level, where responses to cyber attacks are launched, the areas of responsibilities of each one of the institutions involved are not well defined since there is no higher level of authority in the chain of command for cyber power.

The National Defense Policy (PND), approved by Decree No. 5,484, on 30 June 2005, was formulated to protect Brazil mainly against external enemies. It stipulates three strategic fields as priorities: nuclear, space, and cyberspace (MD, 2005).

Given the definition offered by Nelson Jobim (El País, 2009), Minister of Defense from 2007 to 2011—"having a good defense is having the ability to say no when you need to say no"—we conclude that independence in the three strategic areas named above are a basic condition to protect Brazilian national interests in the international arena, the main goal of the PND.

In the nuclear area, we have the National Nuclear Energy Commission (CNEN), a federal agency responsible for

1. assisting in the preparation of the national nuclear energy programs;
2. conducting research, development, and promotion actions related to nuclear power; and
3. providing services in the field of nuclear technology and its applications for peaceful purposes and regulating, licensing, authorizing, monitoring, and controlling such use.

The CNEN acts both in the civilian market and in accordance with military necessities, for example in the Brazilian nuclear submarine project (CNEN, 2014).

In aerospace, we have another federal agency, the Brazilian Space Agency (AEB), which is responsible for formulating and coordinating Brazilian space policy toward autonomy in aerospace, working in collaboration with military and civilian partners (Brazil, 1994).

However, when we look at the cyber defense field, we have a wide range of agencies involved from the executive branch: the Center for Management of Security Incidents in Computer Networks, created in 2006 (GSI, 2006); the Center for Cyber Defense of the Army, created in 2010 (EB 2010); and the Office of Cyber Crimes from the Federal Police, created in 2011 (MJ, 2011), to name a few.

There is not a single federal agency with the full authority to coordinate and formulate issues across the whole federal cyber sector and the sole and exclusive responsibility to ensure the use of national power in the cyber domain. Therefore, we can say that the actions in the cyber domain are now relegated to actors responsible for the actions of other expressions of national power (like the Brazilian Army, which is part of the military expression), but there is no "cyber czar" to act for cyber power specifically.

Another obstacle is that the observed actions focus on the safe use of the global network as the main line of defense, and not on guaranteeing access to the technologies that allow us to access cyberspace (e.g., processors and memory for computers), which certainly leads to a weakening of national power and the inability to provide the security required in the field as stipulated in the PND.

Therefore, we believe that the breakdown of the current system is necessary so that we can use the concepts discussed above, not in a compartmentalized manner as we see today, but with a deductive and holistic view of the subject in order to begin strategic management of the subject. For this to happen, the first step is the classification of the matters that are related to this new expression of national power, called cyber power, because by doing so we will have a defined scope of the environment to start our strategic planning.

Our rationale for the creation of a new expression of national power lies in the fact that, unlike other environments such as space and the seas, cyberspace is an environment created, developed, assisted, and controlled by humans. Therefore, human interaction is necessary for the existence of cyber. Thus we conclude that this environment, so important to civilization, can only be accessed through the mechanisms created by humans, and there are few nations in control of this process of creation.

So if we follow the model proposed by John A. Warden III and we intend to cause a strategic paralysis by a parallel attack or defend ourselves against one (Warden, 1995), we have to be aware that only preparing for a fight in cyberspace (considering a virtual network as a field of battle) is a narrow view of the problem because there is no use having excellent virtual protections in cyberspace if we are denied the opportunity to access it. All our planning will have been useless.

Warden also teaches us that in conflict we should not seek the battle; rather, it is smart to avoid it. We will do this by seeking the enemy's centers of gravity, the elements of its society that directly affect the combat capability of the state. After doing so, we will hit them hard, and the struggle will be brief. So we should not attack them individually, but should simultaneously launch parallel attacks that lead to the enemy's inability to keep fighting and its capitulation in a brief but effective fight.

According to this logic, much more effective than carrying out attacks on the Internet would be using social engineering to attack the humanware in the political expression of national power or exploiting Brazil's total external dependency on the hardware used for all the expressions of national power in just one blow.

Therefore, what we propose as cyber power is a concept that encompasses not only cyberspace but also the ability to access it and the individuals that interact in this environment. This will be possible only if we control the production of equipment (hardware) and the tools used (software) and train those who will work with these two elements (humanware).

Considering that in 2010 we had 16 institutions paying attention to the issue, perhaps some feel that the issue is well covered. However, this author's understanding is the opposite.

This conclusion is based on some assumptions. The first is that no actor has been defined as solely responsible for the development of national policy on cyber defense with the authority to delegate tasks, direct efforts, and produce roadmaps with authority over other public and private organizations. Therefore, there is a lack of leadership at the higher level of national policy decisions.

Another issue is the present lack of defined responsibilities. For example, if a cyber attack hit the electrical grid in a given region of the country, who would be responsible for containment procedures, research of the perpetrators, and, if necessary), retaliation? If we are talking about a crime, we could say that would fall under the federal police, but if we're talking about an act of war, that would be the responsibility of the Army's Cyber Defense Center. This uncertainty raises many other issues:

- For a criminal act, can we accurately identify an individual or organization as responsible?
- For a criminal act, which law applies if the perpetrator performed the act in another country?

- What legitimacy does the Brazilian Internet Bill of Rights have in the international environment?
- Who would be responsible for negotiating the terms of such Bill of Rights in the international community?
- If we classify the attack as an act of war, other issues will pop up:
- What rules apply in the international community to justify our right to declare war (jus ad bellum) in response to a cyber attack?
- Under what rules are we going to fight in the cyber environment while respecting international conventions (jus in bello)?

In the case of a cyber attack embedded in a conventional conflict, who would be responsible for carrying out actions (exploration, defense, and attack) in cyberspace—the Brazilian Army, which would also be involved in conducting ground operations, or a body that would have the sole responsibility of cyber power?

In the examples above, we are seeing only the implications at the state level, but if we move to the private sector, who should protect financial transactions, data communications networks, telephone networks, and the critical infrastructure of high-tech industries? Would the state have this responsibility and, even more, the ability to extend security in these areas?

These challenges are not new and certainly not easy to resolve because they involve many variables, bothinternal and external. As an example of how to deal with these issues, we should look at Harold Valadão's work on aerospace law:

No new power is given to a man without immediate or legal control. It is the duty of the law to protect man against the excesses of other men. For each new social progress, economic or technologic other legal cover for the human person is required. On the threshold of a new era, the rise of a new law (1957, apud FILHO, 2007).

- As for the state's strategic planning regarding cybersecurity, who will answer these questions:
- Is technology independence possible in this sector?
- If not, what alternatives do we have to maintain the security and defense of the country?
- If so, what equipment and systems do we develop and manufacture in the country?
- What are the competencies expected of those who work in cyber defense?
- What is the role of the government, and what is the role of the private sector?

In Figure 1, we can see an example of a proposed unified and interdependent system.

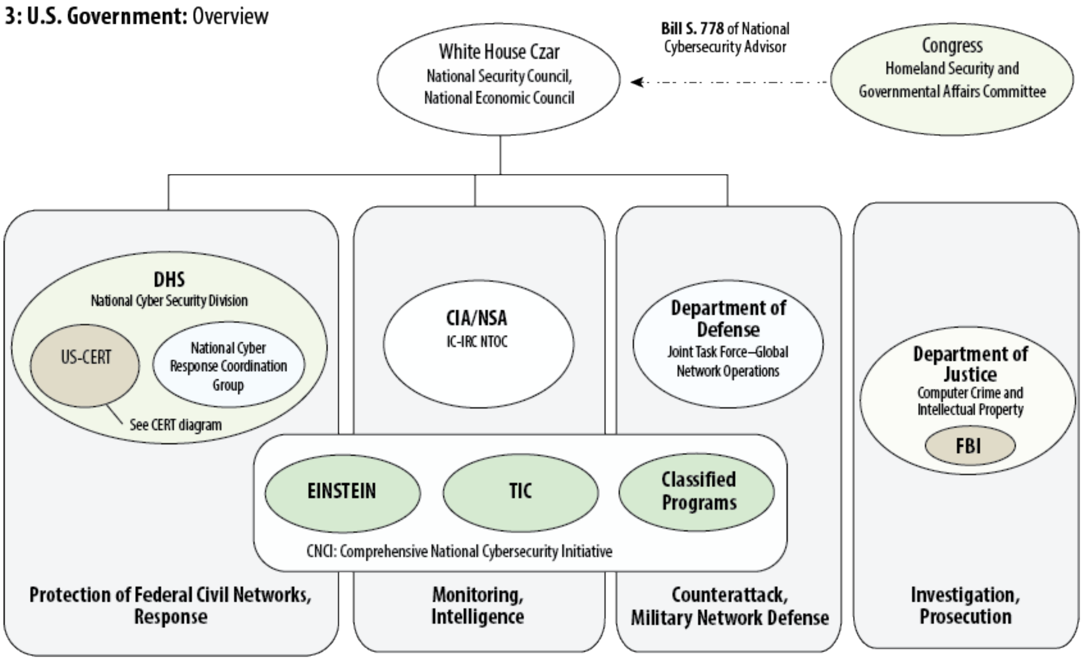

Figure 1. Proposed structure of cybersecurity for the United States (Reprinted from Nazli Choucri, Stuart Madnick, and Jeremy Ferwerda, "Institutions for Cyber Security: International Responses and Global Imperatives," Information Technology for Development 19 (2013): 19, DOI: 10.1080/02681102.2013.836699.

Perhaps this structure is fitted to coordinate efforts in the US Department of Defense, which defines cyberspace as "an interdependent network infrastructure of information technology and data content, including the Internet, telecommunications networks, computers, communications and information systems as well embedded processors and controls" (DOD, 2014).

In our definition of cyber power, we would add to the US definition the organizations that promote research and development as well the regulation of cyber activities (including defense) in both internal and external environments and in the private sector.

Corroborating the ideas presented above, this author believes that defining an actor to exclusively manage strategic policies for cyber operations seems to be not only desirable but an unavoidable solution. But before defining who will pay, we need to define the area of responsibility.

In the methodology that we use, we decided to call this area of activity cyber power, which is a new expression of national power using the concept of ESG. We believe that this action would help future studies by creating paradigms so we can move to the stage of normal science (Kuhn, 1991), where one or more areas could explore the issue either independently or in an interdisciplinary approach.

The definitions we used follow the ones adopted by the ESG:

- Man: the individual or group of individuals with the ability to use an electronic device to interact in a public, private, or mixed networked environment with other members of the web in a relationship of power;
- Earth: the equipment and the operating systems that enable the individual or group of individuals to interact in a public, private, or mixed networked environment with other members of the web in a relationship of power; and

- Institutions: public, private or mixed institutions responsible for sustainability (in the sense of sustentare: to sustain, defend, support, retain) of public, private, or mixed networked environments that allow the man (as defined above) to influence the expressions of national power through earth (as defined above).

Finally, we say that cyber power means the expression of national power that seeks to regulate, control, and develop (in accordance with the moral principles of the society) the transmission of information between individuals and/or social groups as well as the effects of this relationship of power on attaining and maintaining the national objectives.

Conclusion

We have concluded that, in today's society, power relations are changing because of the transformation in the concepts of space and time as well as the substitution of virtual presence for physical presence without a loss in influence in social relations.

Thus, relationships are now increasingly fluid and adaptable to the environment around them, but this comes with an increase in dependence on access to technological equipment, since it is the way we enjoy a totally artificial environment created by humans.

Considering the concepts of ESG, we realize that, in today's world, we cannot discuss security and defense without the ability to project the our national power in the virtual environment (either private or public), and that Brazilian society will not have a sense of security if there is no confidence that our integration into the information age is guaranteed.

It becomes necessary then for us to have the ability to plan our defense in the expression defined by us as cyber power to ensure the safety of our nation against any cyber attack .designed to cause a strategic paralysis, defending ourselves not only in the cyberspace but also outside of it by using national solutions on the hardware and software, for example.

So we found that a good solution would be to establish a new expression of national power and to outline the development of studies, actions, and doctrinal concepts with a holistic view of the situation. We came to the conclusion that an agglutination of efforts would start with the definition of all the actual ideas under a single concept, which we call cyber power.

This congregation of existing concepts is not an evolution of the actual concepts, but a change of the actual reactive system (where we expect a problem to happen and then we try to solve it).

Such a change would occur through the adoption of a deductive point of view, against the current inductive one, with the assimilation of concepts of time, space, and power relations that are completely different from the ones adopted today with the intention of providing a better defense capability to Brazil.

REFERENCES

Bauman, Zygmunt Liquid Modernity Rio de Janeiro: Jorge Zahar Editor .., 2001.

Brazil Army Command -. EB Ordinance No. 666 of August 4, 2010.

Brasilia, Available at:

<Http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C BwQF-jAA and url = http: //www.sgex.eb.mil.br/sistemas/ be / copiar.php? codarquivo ac = 824 & t = & ei = bre meLYU7DOLpLmsATi-

YDYCA and usg = AFQjCNEmEuRHQuBtJgQJGYwSlANIM7sjNA and bvm = bv.71778758, .cWc d>. Accessed: July 22 In 2014.

BRAZIL. Federal Constitution. Brasilia, 1988.

BRAZIL Law No. 8854, of February 10, 1994 Brasilia, Available at:

<Http://www.planalto.gov.br/ccivil_03/Leis/L8854.htm>. Retrieved on July 20 In 2014.

Choucri, Nazli CyberPolitics in International Relations from Cambridge: MIT Press .. 2012.

Choucri, Nazli; Madnick, Stuart; FERWERDA, Institutional Foundations for Cyber Security Jeremy: .. Current responses and new challenges Available on: the July 5, 2014.

CLARKE, Richard; Knake S, Robert CyberWar.'s Next threat to national security and what to do about New York :. HarperCollins, 2010.

Army Command -. EB Ordinance No. 666 of August 4, 2010.

Brasilia, Available at:

<Http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C BwQFjAA and url = http: //www.sgex.eb.mil.br/sistemas/ be / copiar.php? codarquivo ac = 824 & t = & ei = bre meLYU7DOLpLmsATi-

YDYCA and usg = AFQjCNEmEuRHQuBtJgQJGYwSlANIM7sjNA and bvm = bv.71778758, .cWc d>. Accessed: July 22 In 2014.

DEPARTMENT OF DEFENSE - DOD. In:. DOD Dictionary of Military Terms Available at: <hhttp: //www.dtic.mil/doctrine/dod_dictionary/tm> Retrieved June 17, 2014.

Drucker, PF post-capitalist society. 7.ed. Rio de Janeiro: Campus, 1999.

EL PAIS In: "A good defense is Having the capacity To say that the" Madrid, October 28 .. 2009 Available at: <Http://internacional.elpais.com/internacional/2009/10/28/actualidad/1256684401_8502 15.html>. Retrieved July 10 in 2014.

SCHOOL OF WAR - ESG Basic Guide: Fundamentaisv elements .. I.Rio January 2011.

FILHO, José Monserrat The Magna Carta of outer space Available at: .. < http://www.sbda.org.br/artigos/anterior/37.htm> Retrieved July 4, 2014. Institutional Security Cabinet - GSI Ordinance No. April 13 August 2006, Brasilia, Available at: <http://www.ctir.gov.br/sobre-CTIRgov.html#quemsomos> .. Accessed: 22 July in 2014.

GALBRAITH, Kenneth J. Anatomy of power Sao Paulo: .. Pioneer, 1986.

HARVEY, David. condition of postmodernity. Cambridge: Blackwell Publishers, 1989.

KUHN, Thomas. S. . structure of scientific revolutions São Paulo Outlook 1991.

LIBICKI, Martin C .. Cyberdeterrence and cyberwar. Santa Monica: Rand, 2009.

MANDARIN JUNIOR, Raphael. Brazilian defense and security of cyberspace. Recife: Cubzac, 2010.

MINISTRY OF DEFENCE Armed Glossary - MD35-01-G . Brasilia, 2007.

MINISTRY OF DEFENCE. MD30-M-01 Joint Operations Doctrine first volume. Brasilia, 2011.

MINISTRY OF DEFENCE. MD51-M-04 Military Doctrine of Defense. Brasilia, 2007.

MINISTRY OF DEFENCE. national defense policy. Brasilia, 2005.

DEPARTMENT OF JUSTICE -. MJ Ordinance No. 2877, of December 30, 2011.

Brasilia, Available at:

<Http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C B4QFjAA and url = http: //www.dpf.gov.br/acessoainformacao/http___intranet. dpf. gov.br_legislacao_regimento_interno_portaria_n_2-877-2011-

MJ.pdf and ei = qOTYU6LoM8bnsATIqIKACA and usg = AFQjCNG5TOa0NE6nSrVdN-52c3icjc74XA and bvm = bv.71778758, d.cWc>. Retrieved on July 24 in 2014.

National Nuclear Energy Commission - CNEN institutional - Skills Available at: <http://www.cnen.gov.br/acnen/inf-competencias.asp>. Accessed: July 15 In 2014.

Raffestin, Claude . Towards a geography of power São Paulo: Editora Attica, 1993.

VENTRE, Daniel cyberwar andinformation War. London: Iste 2011.

WARDENIII, John A. . Enemy as a System Available at:

<Http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm> Retrieved June 20, 2014.

WEBER, Max Science and politics: two vocations. São Paulo: Martin Claret, 2001.

Captain Luis Eduardo Pombo Celles Cordeiro, (FABRA) (MBA in Public Management-Air Force University – Rio de Janeiro and is a Distinguished Graduate on the class 13 A – SOC -Maxwell AFB) is responsible for the discipline of Military Force Empoyment at the Brazilian Air Force Squadron Officer College (EAOAR)-Rio de Janeiro. He is also responsible for prepare the curriculum of the course as well teaching Air Force Basic Doctrine. Prior to his current job he was the Personal Administration Officer at the 5/8 Squadron–Santa Maria AFB. He is a pilot with more them 3,400 flying hours in the T-25, AT-26, AT-27, C-98, U-42, H-50, H-1H and H-60L.