URVIO, Revista Latinoamericana de Estudios de Seguridad
ISSN: 1390-3691
ISSN: 1390-4299
revistaurvio@flacso.edu.ec
Facultad Latinoamericana de Ciencias Sociales
Ecuador

Gomes de Assis, Camila
The new era of information as power and the field of Cyber Intelligence
URVIO, Revista Latinoamericana de Estudios de Seguridad, no. 20, 2017, pp. 94-109
Facultad Latinoamericana de Ciencias Sociales
Ecuador

DOI: https://doi.org/10.17141/urvio.20.2017.2577

Available in: https://www.redalyc.org/articulo.oa?id=552656641008

Tema central

DOI: http://dx.doi.org/10.17141/urvio.20.2017.2577

Urvio, Revista Latinoamericana de Estudios de Seguridad, No. 20, Quito, junio 2017, pp. 94-109
RELASEDOR y FLACSO Sede Ecuador • ISSN 1390-4299 (en línea) y 1390-3691

The new era of information as power and the field of Cyber Intelligence

La nueva era de la información como poder y el campo de la ciberinteligencia

Camila Gomes de Assis[1]

Date of receipt: February 13, 2017
Date of acceptance: April 20, 2017

Abstract
This article seeks to describe the interference of cybernetics as a key intervening factor in the consolidation of information as a power resource in the 21st century. Aware that information is the main substrate for the practice of intelligence, the studies carried out also seek to understand the transformations generated by the inclusion of cyberspace in this practice, highlighting how the particular characteristics of this domain are responsible for generating new demands to States in terms of defense and security. In order to achieve the proposed objectives, this paper is structured into three main discussion topics. The first one will hold a brief discussion about the particular characteristics of this new domain and its political significance to International Relations. The second topic will deal directly with the issues of intelligence and an evaluation of the interference of cyberspace in the intelligence practice will be carried out focusing on the study of the North American - dedicating a third topic to such discussion. In methodological terms it is a descriptive work; therefore, it will be guide by the analysis of international events that approach this subject, as well as by the literature that dedicated to such discussions. This article does not seek to end with such questions, but to present itself as a north to future discussions on this subject.

Keywords: Cyberspace; Cyber-Intelligence; International Relations; Power.

Resumen
Este artículo pretende describir la interferencia de la cibernética como un factor clave para la consolidación de la información como recurso de poder en el siglo XXI. Conscientes de que la información es el principal soporte para la práctica de la inteligencia, los estudios realizados también buscan comprender las transformaciones generadas por la inclusión del ciberespacio en esta práctica, destacando cómo las características particulares de este ámbito son responsables por generar nuevas demandas a los Estados en términos de defensa y seguridad. Con el fin de lograr los objetivos propuestos, este documento se estructura en tres temas principales de discusión. La primera tendrá una breve discusión sobre las características particulares de este nuevo dominio y su significado político para las Relaciones Internacionales. El segundo tema abordará directamente las cuestiones de inteligencia. Una evaluación de la interferencia del ciberespacio en la práctica de inteligencia se llevará a cabo centrándose en el estudio de los norteamericanos - dedicando un tercer tema a dicha discusión. En términos metodológicos es un trabajo descriptivo; por lo tanto, será guiado por el análisis de los eventos internacionales que abordan este tema, así como por la literatura dedicada a tales discusiones. Este artículo no pretende terminar con tales preguntas, sino presentarse como un norte a discusiones futuras sobre este tema.

Palabras clave: Ciberespacio; Ciber-Inteligencia; Relaciones Internacionales; Poder.

1 Master's Degree in International Relations for the Postgraduate Program Santiago Dantas (Unesp, Unicamp, PUC-SP - Brazil). Graduated in International Relations from Universidade Estadual Paulista (UNESP), Brazil. Researcher at the Defense and International Security Studies Group (Gedes). E-mail: camilagomesdeassis@gmail.com

Introduction

In June 2013, Edward Snowden, a former employee of the US National Security Agency (NSA), reported, with contribution from the journals *Washington Post* and *The Guardian,* confidential information responsible for reveal a national and international surveillance scheme carried out by the US government. This surveillance was implemented through the usage of a program entitled PRISM.[2] This program was responsible for conducting a rigorous monitoring of the North American citizens and the international community through internet access. Counting for this with the collaboration of large social media companies like *Facebook, Microsoft, Apple, Google* and *Youtube*.[3]

According to information disclosed, the volume of data in the possession of the US government is huge. Almost all of the information exchanged on the Internet, such as emails, videos, photos, and browsing history were under the disposition of the United States government. The statement that international leaders were also under US surveillance, like the Brazilian president Dilma Rousseff and the German Chancellor Angela Merkel, generated a great international repercussion.[4]

Multilateral forums such as the UN were place within which gained relevance the discussion about the need to devise new mechanisms that would allow States to protect information considered confidential and strategic to maintain their stability and promoting their interests in an international environment. The discussion about the need to preserve human rights in this new domain also gained prominence.[5] In a resolution signed in November 2013, under the coordination of Brazil and Germany, during the UN General Assembly, was declared that

> […] illegal surveillance of communications, their interception, as well as the illegal collection of personal data constitute a highly intrusive act that violates the right to privacy and freedom of expression and may threaten the foundations of a democratic society (UN 2013, 2)

Reaffirming:

> the human right of individuals to privacy and not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence, and the right to enjoy protection of the law against such interferences and attacks, and recognizing that the exercise of the right to privacy is an essential requirement for the realization of the right to freedom of expression and to hold opinions without interference, and one of the foundations of a democratic society (UN 2013, 1).

Based on the above mentioned, it is observed that the episode in question, and the international convulsion generated by it highlighted

2 This information has been removed from: Black, Ian. 2013. "NSA spying scandal: what we have learned". The guardian, 10 june. https://www.theguardian.com/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned.

3 This information has been removed from: Greenwald Glenn, Ewen MacAskill y Laura Poitras. The 2013. "Edward Snowden: the whistleblower behind the NSA surveillance revelations". The guardian, 11 june. https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

4 This information has been removed from: Ball, James. 2013. "NSA monitored calls of 35 world leaders after US official handed over contacts". The Guardian, 25 october. https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

5 This information has been removed from: BBC News, 2013. The UN General Assembly adopts anti-spy resolution.,http://www.bbc.com/news/world-latin-america-25441408.

a fundamental question: the fact that the practice of collecting confidential information in order to build strategies favorable to a given State is not a new practice, however, its use through cyberspace is. Leading, consequently, to transformations *in the manner in which* and *in the intensity with which* this activity is performed (Nye 2010, 3). Conducing to the emergence of new challenges to States in all fields, including security and defense issues (Lopes 2013). In this way, it can be affirmed that the Information Revolution of the 20th century, based on rapid technological advances in computers and communications, only collaborated to consolidate information as a fundamental strategic asset to the States, reshaping the use of this resource (Minc y Nora 1981; Libick 2009; Kello 2012).

The Information Revolution described was responsible, therefore, for promoting extraordinary declines in the costs of creating, processing, transmitting and searching information (Nye 2014). Leading not only to changes in the forms of social and individual interaction as pointed out by sociologists Manuel Castells (1999) and Pierry Lévy (1999), but also in the dynamics of interstate relations, such as Nye (2010), Clark and Knake (2010), John Arquill a and David Ronfeldt (1993) and Libicki (2009)[6] pointed out. The changes associated with the emergence of these new technologies conduce to the conformation of a new domain: cyberspace, within which international practices will be remodeled in terms of power (Libicki 2009).

In this sense, as the Information and Communication Technologies (ICTs) revolution spreads around the globe, it modifies the way we do business and conduct policy between and among nations, changing, according to Nye (2010), the nature of Intelligence, opposition politics and war. The present article will focus on the studies of this interference within intelligence activities. In this way the central objective of this work is to describe the influence of the so-called New Technologies of Information and Communication (NICT), represented here by the inclusion of cyberspace, within the National Intelligence Services, presenting the new challenges and threats imposed to the practice of intelligence, and therefore to the role played by information as an instrument to exercise power in the 21st century.

In general terms, it is intended to briefly conceptualize what cyberspace is, its general impact on international dynamics, and, finally, to focus on the issues that debate its interference in the practice of intelligence. In view of the intentions presented, the article is structured into three main discussion topics. The first one will hold a brief discussion

6 For a better understanding of the interference of cyberspace to the practice of International Relations it is recommended to verify such authors: (I) Joseph Nye in his work "*Cyberpower*" (2010) seeks to describe what cyberpower comes to be and how this kind of power, with particular characteristics, inserts within the struggle between nations in international environment.. (II) Clark and Knake wrote the book "*Cyber War: the nex threat to national security and what to do about it*". This work is centralized in the discussion about the incorporation of cyberspace to North American policy, focusing on the interference of this element within the practices of defense and security policies. (III) The book ""*Cyberwar is coming!*" written by John Arquilla and David Ronfeldt (1993) manifests itself as one of the primary literatures in addressing cyberspace in International Relations. The focus given to the author is on the interference of the cybernetic element in the conduct of war practice. (IV) Finally, Martin Libicki (2009) in his book "Cyberdeterence and Cyberwar" carried out an in-depth analysis of the interference of cyberspace with the practice of defense and war by states. Behaving as an author of fundamental importance to those who want to dwell on such studies.

about the particular characteristics of this new domain and its political significance to International Relations. The second topic will deal directly with the issues of intelligence and third topic will be dedicated to an evaluation of the interference of cyberspace in the intelligence practice focusing on the study of the North American case.

The choice of The United States as an object of analysis is justified due to the country's tradition in using technological means as an instrument to construct offensive and defensive power in the international arena (Bretton 1991; Almeida 2006). The United States is one of the first countries to give relevance to cyberspace highlighting even the interference conducted by this new domain into intelligence practice (Clark y Knake 2010). According to the official US document entitled *International Strategy for Operating in Cyberspace* (2011), the north American perception of vulnerability and opportunities imposed by the cyber domain highlights the need to employ new operational concepts of defense, including a more active cyber defense (capable for protecting the networks) allied with the development of more expressive cyber intelligence departments able to meet the new demands imposed by technological transformations in world (United States 2011, 1).

So, the relevance of the proposed discussion is evidenced, mainly due to the growing importance attached to the use of electronic communication and, therefore of cyberspace, as a primary tool to purchase Intelligence and attacking the opponent's decision-making power without the use of force within the contemporary international scene (Hare 2009). Regarding the choice of theoretical contribution, the realistic perspective was chosen to guide the reflections proposed by this paper. The realists, from classics to neorealist, usually understand international relations in a deterministic way having as a key concept to their interpretation the idea of power (Herz 1951). Among the central foundations of realism, we can also mention (i) the perception of the predominance of competition and the conflictive dimension on all forms of relations between international actors, and (ii) the concern for security as one of the great conductors of states's action (Morgenthau 1985; Vigevani, Veiga y Mariano 1994). In this way, states towards the international structure live "in the shadow of war" (Aron 1986, 52). This implies a constant contest for power, especially in the form of military power, although other forms are also possible.

The focus on the political-military dispute therefore places activities such as the practice of Intelligence by States in a position of fundamental relevance to understanding the dynamics of international relations. This practice, therefore, highlights the role of power, the need for competition, and the needs for change through the promotion, for example, of technological advancement. It is known that the Realism has interpretative gaps, since it neglects social, cultural or even economic aspects, giving exacerbated value to political-military aspects; however, is exactly this simplification that leads us to choose such theoretical side. The choice of a theoretical strand that prioritizes the political-military element helps us understand the inclusion of cybernetic issues in International Relations. Due to the current relevance of this theme and the multiple factors surrounding its understanding, it is believed that focusing on an approach that prioritizes power, and military aspects, is positive for the proposed goal. So, understanding cybers-

pace by the realistic theoretical side, allows us to interpret this as a new operational domain within which states systematically seek to increase their cybernetic capacities with a view to maximizing their Power (Acacio y Lopes 2012).

The construction of a new domain: the cyberspace

According to a technical definition, cyberspace corresponds to an operational domain marked by the use of electro-electronics and the electromagnetic spectrum for the purpose of creating, storing, modifying and exchanging information by interconnected and interdependent networks (Kuehl 2009, 29). Based on this is possible to affirm that telegraph networks, amateur radio, mobile telephony and satellite television shaped cyberspace long before the advent of the Internet (Blumenthal y Clark 2009, 206). However, it is since the scientific-technological revolution of the 1970s that such networks started to rely on information and communication technologies (ICTs) focused on computing, among which the advent of the internet stands out (Castells 1999).

Over the years, through Internet's popularization, it has become not only the main network that makes up the cyberspace, but the platform to which other technologies have converged (Bretton 1991). In this sense, when we argue about cyberspace, we often refer to the transformations caused by the inclusion of the Internet in its scope, which was responsible for eliminating the physical limitations of time and space, including in conducting military attacks (Gama Neto y Lopes 2014, 29). According to Nye (2014) the key characteristic of this recent information revolution, and consequently of this new domain, is not the speed of communications but the considerable and very significant reduction of costs for transmit, process and access information.

For all practical purposes, transmission costs have become negligible leading to a significant increase of the amount of information that can be transmitted worldwide. The cheapening of these processes made possible an expressive increase in the number of individuals that have access to this system. The popularization of this technology has undeniable political implications (Nye 2014). In the field of International Relations, we observe that the internet empowered individuals in previously unimaginable ways. Conducing, in consequence, to an increase in the number of actors responsible for influencing the international political game (Arquilla y Ronfeld 1993; Nye 2010; Hare 2009).

In contrast to the physical world, where states have the legitimate monopoly of violence and attacks are extremely costly because of the high cost of resources used, the cyber world allows overcome this physical limitations of time and space, allowing actions and attacks be executed with effectiveness and to lower costs for anyone who has an internet-connected device (Nye 2010). In a practical assessment of the international scene, focusing our evaluation on episodes that specifically involve the use of information as a transforming aspect to the power game, we can identify a series of new actors. Wikileaks, the Anonymous movement and the self-styled "the jester"-people who act alone thanks to their advanced technological mastery- often have technological capabilities comparable to many countries, presen-

ting an undeniable directly or indirectly relevance in international politics (Kuhl 2009). The inclusion of new actors, makes the international dynamic even more complex and uncertain, generating new demands for the national defense, security and intelligence sectors (Libicki 2009).

Another transforming feature of international dynamics, is the fact that cybernetics knows no boundaries, so attacks can come from distant, undisclosed locations. This, in turn, renders the international environment more "uncertain" given the difficulty in assuming responsibility for the acts practiced in this fild (Nye 2010; Libicki 2009). It happens because "most of the suggestions regarding nation states involvement in cyberattacks against other countries are generally inferred from circumstantial rather than direct, factual and conclusive evidence" (Kshetri 2014, 4). Or even if such origins are established many questions arise regarding the attribution of responsibilities. For example, if an individual in the North American territory attacks the physical infrastructure of a particular country through their computer, how is possible to determine whether it was an individual attitude or even a state-funded? This difficulty in assigning responsibilities, inevitably leads to more insecurity once they break with the constraints.

In addition, authors such as Nye (2010, 1) affirm that the ease access to cyberspace can lead to a possible change in the balance of power, because it can promote the reduction of power differences between countries, promoting a greater diffusion of the potential for state acting in the international system. It is imperative to point out that this diffusion of the potential of international action does not necessarily translate into an equality of power between nation-states. Countries such as United States continue to occupy a privileged position within international dynamics, adding to their kinetic military resources the use of technological instruments in the promotion of their economic and military power (Nye 2010).

Also based on the technical aspects involved in the conformation of the cyberspace, it is known that this in opposition to the other domains - terrestrial air and sea - is not a natural domain but created by man himself (Sheldon, 2014). This space differs from others in relation to interconnectivity. For Ventre (2011), the cybersapce transcends all the others. Through this argument, Ventre (2011) explains that there are several access points to the cyber space in the other geographical spaces, and in a similar way, according to the author, through cyberspace influence can be exerted on the other domains. In this way, actions performed in a virtual environment can generate consequences in physical environments. This possibility of diffusion of power from the virtual medium to the physical is called transversality (Ventre 2011).

Transversality as a particular feature of the fifth domain –cyberspace- is responsible to allow the projection of cybernetic power and its reflections on other domains of state action: land, sea, air and space). On the basis of the foregoing, there is now a growing vulnerability of the physical domain of states to cybernetics, since the safety and effectiveness of the operation of a wide variety of critical and strategic national infrastructures such as energy, finance, transportation, banking negotiations, communications and intelligence and security services are directly linked to and dependent on this domain (United States 2011).

Recent episodes from Estonia (2007)[7] and Georgia (2008)[8], illustrate this fragility, evidencing the strong impact of the transversality of the cyberspace in national physical infrastructures. It is observed, therefore, that the broad technological development can also lead to disadvantages. The more technologically developed nations with greater potential for cyber attack, also become the most vulnerable, since they have a greater dependence on the technological element. In light of this, cybernetics provides to states not only a greater variety of instruments to be used as resources of power, but also increases the vulnerability and instability present in the international system (Sommer y Brown 2011; Nye 2010).

Authors like Clarke and Knake (2010) affirm, from a realistic conception of this phenomenon, the undeniable presence of the possibility of new forms of conflict in the cyberspace, giving rise to the so-called "cyber wars". According to these authors: (i) cyber war is real; (ii) cyber war happens at the speed of light; (iii) cyber war is global; (iv) cyber war skips the battlefield, and (v) cyber war has begun (Clarke y Knake 2010, 30-31). On the other hand, authors like Peter Sommer and Iann Brown (2013) maintain that the great variety of events classified as cyber war represent an wrong use of the concept, since there will hardly be a purely cybernetic conflict. Despite the divergent opinions on the possibility of a purely cybernetic war, nowadays, it is possible observe, with some homogeneity, the importance attributed to cyberspace and its associated practices. Numerous countries have attached importance to these issues within their defense and security policies.

Using as an example the North American case, we observe an increasing valuation of cybernetics -and cyberspace- as a fundamental strategic component in promoting the interests and preservation of US national sovereignty since Obama's administration. At the same time is possible to identify an intensification of a discourse within which cybernetic is detected as a threat, affirming the character of urgency and danger directly associated with those issues (Jentlenson 2010). As can be seen in the section to be presented, the US government puts itself in a position of vulnerability, evidencing, after analysis, the strong deficiencies present in the defense structures and cybernetic security characteristic of the US:

> The architecture of the Nation's digital infrastructure, based largely upon the Internet, is not secure or resilient. . Without major advances in the security of these systems or significant change in how they are constructed or operated, it is doubtful that the United States can protect itself from the growing threat of cybercrime and state-sponsored intrusions and operations (United States 2009, 1).

7 On 27 April 2007, Estonia suffered a series of cyber attacks through the DoS - denial of service attack. The Estonian government accused Russia of having motivated this attack. The allegations against the Russian government have not been proven because of the unknown origin of the attacks. The attack on Estonia's infrastructure is considered the first major cyberattack within the international relations. For more information access: Shetter, L. 2007. "Estonia Accuses Russia of" Cyber Attack "to the Country". BBC, May 17. Available in <http://www.bbc.co.uk/en/reporterbbc/story/2007/05/070517_estoniaataquesinternetrw.shtml>

8 In 2008, during a period of tension between Russia and Georgia, hackers promoted DDoS Attack (Short for Distributed Denial of Service) in order to overload Georgia's Web sites and servers in the weeks leading up to the military invasion. In the region. For more information about the épisodio consult. LEE, D. 2014. Russia and Ukraine wage "cyber-duel". BBC Brazil, 7 March. Available in http://www.bbc.co.uk/portuguese/noticias/2014/03/140307_russia_ucrania_bg.

So it is not surprising that governments express their intention to defend the strategic assets and interests of their countries in this area, seeking to acquire greater offensive and defensive power within this domain, in particular by reformulating their intelligence and Counterintelligence affecting directly the politics of security and defense of States (Gagnon 2008; Lopes 2013). The new demands imposed on states in political and military terms translate, therefore, into an increasing preoccupation to promote a cybersecurity and cyberdefense policies. Cybersecurity, as Gills Lopes (2013, 27) points out, "refers to the combat and prevention of so-called cybercrimes in the sphere of public security, and is therefore under the responsibility of police forces or even public ministries".

Cyberdefense, on the other hand, refers to the military sector, being "the set of defensive, exploratory and offensive actions in the context of a military planning, carried out in cyberspace" (Carvalho 2011, 8; Lopes 2013). It is assumed, then, that cybernetic defense means, according to Lopes (2013) to safeguard national security against cyber existential threats. Both cybersecurity and cyberdefense rely on intelligence and information security practices. In this way the changes generated by this domain become fundamental to describe the new configuration of the International Relations.

Intelligence in International Relations

Before entering the debate about the interference of cyberspace in the practice of Intelligence, we need to rescue its role in International Relations. As mentioned earlier, since the earliest times information has played a fundamental role in the struggle for power among nations, so intelligence has always been playing a fundamental role for the States in the process of conquering their interests and objectives. In general, the practice of Intelligence can be defined as:

> [..] that component of the struggle among nations that deals with information. Intelligence seeks to learn all it can about the world. But intelligence can never forget that the attainment of the truth involves a struggle with human enemy who is fighting back and that truth is not the goal but rather only a means toward victory (Shulsky 1992, 197).

When we look at the literature that deals with the role of Intelligence applied to the international scene, we can understand this activity through three different meanings: a type of information, a peculiar activity or as a type of organization (Costa Júnior 2011, 13). As outstanding Michael Herman:

> Inteliggence in government is bade on the particular set of organizations with that name: (i)"the intelligence services" or "intelligence community". Intelligence activity is what they do(ii), and intelligence knowledge, what they procude (iii) (Herman 1996, 2).

In terms of conceptual definition, intelligence as an organization is defined as a sort of state agency based on secrecy and which product, although it rewards the benefit of society, is not accessible to the citizens (Costa Júnior 2011). As important as understanding the definition of such concept is identify its usefulness in practical terms in state policies. Thus, taking over Cepik's

(2003) and Costa Júnnior's (2011) studies, one can conclude that governments have national intelligence services with the purpose of supplying eight utilities, namely (1) contributing to transform the governmental decision-making process more realistic and rational; (2) establish a process of interaction between decision makers and intelligence officers with cumulative effects; (3) give support to defensive planning capabilities and the development of the acquisition of systems and weapons; (4) obtain relevant information through diplomatic negotiations in various areas; (5) ability to subsidize military planning and the preparation of war plans; (6) anticipation of possible counterattacks by alerting civilian and military officials; (7) monitoring of priority targets and external environments, thereby reducing uncertainty and increasing knowledge and confidence; (8) preserving secrecy about the informational needs of its adversaries.

When we talk about intelligence as (ii) a type of information we can describe intelligence as all information collected, organized, analyzed and submitted to a special process of elaboration that aims to meet the demands of a decision maker (Cepik 2003; Sims 1995). Through this definition we can deduce that the basic objective of intelligence is the production of a specific knowledge for decision makers who aim to increase the probability of a correct decision and therefore the advantages over the opponent (Sims 1995, 4).

As an activity, intelligence will act in an environment where secrecy behaves as a fundamental factor, marking the competition between those states that don't want their knowledge, activities or actions to be discovered while, at the same time that they seek to acquire as much as they can about other states confidential information. So, "Intelligence as an activity may be defined as that component of struggle between adversaries that deals primarily with information" (Shulsky 1992, 2). It is, therefore, envisaged that intelligence activities simultaneously seek to obtain information from other actors at the same time as it is necessary to protect and neutralize the enemy's abilities to obtain relevant information about the functioning of the state in question. In this way, it is essential to maintain the security of a wide range of sensitive information by governments, in this context gained relevance the practice of information security (Herman 1996, 165). As Cepik points out:

> [...]The information security area seeks to protect information that, once obtained by an adversary or enemy - for example through the intelligence operations of a foreign government - could render the state and citizens vulnerable and insecure (2003, 20).

Thus, the Intelligence refers not only to espionage activities or information, but to certain types of information that are related to the defense of the State; Counterintelligence and other organizations that are responsible for conducting and coordinating this activity at the state level(Sims 1995). Being characterized, therefore, by the acquisition, analysis, processing, production and dissemination of data that are used in the area of foreign policy and national defense. The focus of this work is precisely to point out how a greater dependence on technology -with the inclusion of cyberspace- allows at the same time a greater efficiency by the States in practicing Intelligence - being able to enter more easily through computer programs in confidential files of other countries-, and either the expan-

sion of their vulnerabilities due to imposing new challenges to the practice of counterintelligence, because the opposite also happen with them, it means other states can access their system easily. Such issues will be further explored in the subsequent topic. In this way, the influence that cyberspace will exert on this practice and on its utilitarian effects on the State is visible. So, the aim of this paper is precisely to point out these transformations, focusing more precisely in the definition of Intelligence as a practice (ii).

The intelligence services in the face of technological transformations: the cyber intelligence

Throughout the centuries, the use of secrecy, or in other words, the information in a confidential way, was considered a fundamental element for the art of governing (Bessa 1996). Important strategists such as Sun Tzu, since long ago, have highlighted information as a key factor for States achieve victory in the War. In his classic work *The art of War* Sun Tzu (2007) obviousness the importance of the employment of spies. According to the Chinese general:

> […] what enables the wise sovereign and the good general to strike and conquer, and achieve things beyond the reach of ordinary men, is foreknowledge. That is, knowledge of the enemy's dispositions, and what he means to do. This foreknowledge cannot be elicited from spirits, and cannot be obtained inductively from experience, nor by any deductive calculation. Knowlegde of the enemy's dispositions can only be obtained from other men […] (Sun Tzu 2007, 150).

However, over the years, is possible to notice a transformation in the role of information as a power resource to states. In a historical perspective, the end of World War II and the emergence of an ideological political dispute during the Cold War led the activity of Intelligence from the level of practice merely focused on military campaigns to a resource with fundamental importance for the security and development of states (Dandoneli, Giovani de Paula y Souza 2012). Giving to information a political meaning that transcends the battlefield (Andrew 1998). During this period was possible to observe the creation of ministries and services dedicated exclusively to the execution of such practice (Fernandes 2012, 22).

Permeating this transformations, technology has always been linked to the Intelligence activity being responsible for allowing a greater access to privileged information as well as greater effectiveness in the formulation of strategies to those who obtain a high technological development (Dandoneli, Giovani de Paula y Souza 2012, 120). The emergence of the computer, for example, is associate to the power struggle between nations (Brito 2011, 21). The creation of the first prototype by Alan Turing - the father of computer science and artificial intelligence - relates to British intelligence efforts to decipher, at the time of World War II, the messages generated by the German Enigma machine. The aim was to decode the German messages in order to take knowledge of the Germany strategies in war and consequently take actions that enables the allies to win.

The creation of ARPANet, a forerunner to the Internet, is also associated with the strategic importance of technological development in the international power struggle held during the Cold War, through the US Agency

for International Development (DARPA) (Bretton 1999). This enterprise arose from the need to create a network of communications inviolable to possible Soviet attacks. Allowing the United States to preserve, within its Intelligence Services, information considered fundamental to the promotion of its interests and the maintenance of national security (Bretton 1999; Castells 1999; Lojkine 1995; Minc y Nora, 1980).

In the face of these findings, Intelligence must be understood as a complex adaptive system in which the processes of construction, production and management of information and knowledge are able to be optimize through the technological increment at the domestic and international (Dandoneli, Giovani de Paula y Souza 2012). Therefore, the role played by cyberspace can not be denied as an important element in the practice of Intelligence. In this scenario, it is observed the emergence of new information access strategies, such as the Computer Network Exploitation (ERC) practice, as well as new mechanisms capable of compromising the technological tools of the opposing Intelligence systems, undermining their ability to collect information considered fundamental to the promotion of security and the projection of their national interests (Machado 2010).

As a result of the emergence of these new doors of vulnerability, States are obliged to maintain the integrity of their computer networks and systems not by means of physical defenses, such as the use of the armed forces, but by reducing vulnerabilities in their systems to protect their data (Bajaj 2010, 2). Among the cyberweapons used to carry out such a practice are (i) the use of viruses responsible for contaminating executable files of the critical infrastructures of adversary states; (ii) SQL Injection, defined as changing the database access commands; Denial of Service attacks, which are responsible for rendering a system's resources unavailable to its users and, finally; (iii) the Computer Network Attack (ARC) responsible for damaging, denying, corrupting, degrading or destroying critical infrastructure of adversary countries, as well as the information contained therein or the systems controlled by them (Gama Neto y Lopes, 2014).

In addition to these procedural factors, the emergence of a growing demand for more efficient processes of information sorting and storage, caused mainly by the increase of the information flow and the ease access to information, made possible by the Internet connection, generate new problems to be faced by the State (Dcaf Backgrounder 2008, 3). This new challenge appears because intelligence and security services have generated a lot of data to be classified. However, the collection of information does not automatically translate into better results in the decision-making process. Even when important information is available, locating them and recognizing their importance in time to prevent disasters can be a challenge (Nye 2010).

An example, is the transformations in the treatment of the ostensive sources, or open sourcers intelligence (OSINT). This kind of intelligence derives from obtaining public information about political, military and economic aspects of the internal life of other countries or targets in a legal, direct and non-clandestine way through the monitoring of the media (newspapers, like BBC/ Le Monde Diplomatic and other national and local journals; radio and television). The advent of the Internet and the greater connectivity generated by it, generating even more information

to be processed and transformed into intelligence (Machado 2010).

There is, therefore, a clear transformation of Intelligence into its operational process, that is, as a data collection and search procedure, since the effectiveness of the intelligence services is directly related to the process of development and improvement in the production, procurement, management and transmission of informations considered strategic to the States (Cepik 2003; Gama Neto y Lopes, 2014). However, obtaining information about the States, the organizations or the individuals is not limited merely to public and OSINT. The activity of intelligence also included access to confidential informations (Cepik 2003). So, the cyberspace also opening space for the intensification and transformation of the espionage practices. The international conjuncture itself evidences this process. The denunciations by Julian Assange and Edward Snowden emphasizes the use of this new instrument as a transformer of the use of an old resource to the International Relations: the information.

Recapping these episodes, the Wikileaks website, founded in 2006 by Australian cyberactivist Julian Paul Assange, gained international visibility by publishing a series of secret documents produced by the US government (Harding y Leigh 2001). The so-called *Cablegate project* made public about 251,287 diplomatic communications from 247 US embassies around the world. Among the various accusations was the charge about espionage practice by the US government, such as Secretary of State Hilary Clinton's requests to 33 embassies and consulates for diplomats doing a vigorously monitoring of the representatives of Various UN countries (Assange, Appelbaum, Maguhn y Zimmermann 2013).

In 2013 it was Edward Snowden's turn as mentioned at the beginning of this article. The episode in question was responsible for generating a great tension between the United States and the international community, especially with Germany and Brazil, as these countries obtained the privacy of their heads of government, Chancellor Angela Merker and President Dilma Rouseff, respectively, violated by US intelligence agencies. In view of this, there is, therefore, a constant attempt to improve security in this domain, gaining relevance due to this the practice of Information Security, defined as an activity responsible for protecting information considered strategic to the State and which, if obtained by its opponents or enemies, may make the country and its citizens vulnerable (kent 1967, 9).

This practice consists of three practically autonomous activities: Counter Intelligence, Security Countermeasures (SCM) and Operations Security. The emergence of a new domain and resource to be used by the states (cyberspace) makes it fundamental, in turn, the association of these activities with the implementation of a cyber-security, defined, according to the Technical Group on Cyber Security, linked to the Security Office (Brazil 2011, 45) as the "art of ensuring the existence and continuity of the Information Society of a Nation, guaranteeing and protecting, in the Cyber Space, its information assets and its infra- Structures". Countries such as Brazil and the United States have already moved toward implementing national cyber security systems (Miles 2016; Machado 2010).

The United States, the major world power in the world, has identified as necessary create a new Intelligence Agency entitled *Cyber Tread Intelligence Integration Center (CTIIC)*, dedicated exclusively to the practice of cyber

security. CTIIC will work seamlessly with other US intelligence services, such as the FBI, the CIA and the NSA, with the primary goal of ensuring cyber security in the country (United States, 2011). Finally, it is important to consider that the interference of the technological element within the practice of Intelligence leads to an intensification of the use of information as a soft power resource by the countries , given the greater speed in the transmission of information and the connectivity provided by the Internet.

These operations are called covert operations and it aim to influence a foreign "audience" which could be a government, government leaders, the population of a nation, a segment of the population or even non-state groups like terrorist organizations, to do something (or fail to do something) according to the interests of the foreign policy of a particular country, creating a change of behavior (Cepik 2003). This kind of Intelligence to be effective demands that activities conducted are viewed as legitimate by the target audience. In the field of cybernetics, this practice takes place through secret intrusions into computer databases for the purpose of altering or destroying computer hardware, software, or information (Miles 2016; Arquilla y Ronfeldt 1993).

Differentiating, therefore, from secret invasions that aim only to learn what information consists of, without altering or corrupting the data (Cepik 2003). Countries such as the United States, for example, are often able to be present through public diplomacy, propaganda, psychological campaigns with greater ease in a greater number of countries, intervening in a direct way about the capacity of perception of the reality of one people or of rulers considered opponents. In this context, once again the Internet has gained prominence in giving greater speed and scope to the political and cultural subversion practiced by these intelligence agencies. Accelerating the impact of policies across the globe.

Conclusion

Face of the reflections made during all this paper, we conclude that the influence of cyberspace on the practice of Intelligence in the 21st century is relevant. Due to the particular characteristics of this domain, marked by a greater number of actors, the ease access in this field, its transversality and at the same time the difficulty in imputing responsibilities, a new number of challenges and opportunities rise to modify an old practice, which is the use of information in order to purchase power. Faced with this new scenario, not only States but also individuals and organizations can become a threat to be faced, because everyone with a computer can be a potential enemy. All this new structure of the relations derived by the cyberspace, is responsible for generating several questions that are still little explored and that don't have precise answers.

One of the question which could be made is: *How we could differentiate the so-called information war, presents since the most remote times, of the so-called cyberwars, a new form of conflict originated from cyberspace?* The States itself treat these issues in a still very confusing way, but we can not disregarding the political intention by this way of acting. Some countries like United States is safeguarding the right of an offensive stance, in the face of cyberspace, hidden, however, by a defensive discourse (Jentlenson 2010). The insecurity

attributed to this domain sets the precedent for this country to legitimize more assertive actions, under the pretext of defending national interests and sovereignty, following the Weberian maxim of the legitimate use of force for the preservation of the nation-state (Lopes 2013; Machado 2010). All this just show us the relevance of cybernetics in the International Relations and as presented by this paper the undeniable relevance of this new domain to the practice of Intelligence.

References

Acácio, Igor, y Gills Lopes. 2012. "Segurança internacional no século XXI: o que as teorias de Relações Internacionais têm a falar sobre o ciberespao?". *Encontro Anual da Anpocs* 36.

Almeida, Fernando C. 2006. "Poder americano e Estados Nacionais: uma abordagem a partir das esferas econômica e militar" (tesis de maestria de la Universidade Federal de Uberlândia).

Andrew Christopher, 1998. "Intelligence and International Relations in the Early cold War". *Review of International Studies*: 321-330.

Aron, Raymond. 1986. *Paz e guerra entre as nações.* Brasília: UNB.

Arquilla, John, y David Ronfeldt.1993. "Cyberwar is coming!". *Comparative Strategy* 12 (2): 141-165.

Assange Julian, Jacob Appelbaum, Andy Müller-Maguhn y Jérémie Zimmermann. 2013. *Cyberpunks: Liberdade e o Futuro da Internet*. São Paulo: Boitempo.

Bajaj, Kamlesh. 2012. *Cyberspace as Global Commons: The Challenges*. India: Dataquest India.

Bessa, António Marques. 1996. *A Arte de Governar. Ensaios sobre a Classe Dirigente e a Fórmula Política.* Lisboa: SCSP.

Blumenthal, Majory S., y David Clark. 2009. "The future of the Internet and cyberpower". En *Cyberpower and National Security*, editado por Franklin Kramer, Stuart H. Starr y Larry Wentz, 206-240. Washington, D.C.: National Defense University Press.

Brasil. 2012. *Livro Branco de Defesa Nacional*. Brasília: Presidência da República. http://www.defesa.gov.br/arquivos/2012/mes07/lbdn.pdf.

Bretton, Philippe.1991. *História da Informática.* São Paulo: Editora da Unesp.

Clarke, Richard, y Robert K. Knake. 2012. *Cyberwar: The Next Treat to National Security and What to Do About It*. Nova Iorque: Harper Collins.

Carvalho, Paulo Sergio M. de. 2011. "A defesa cibernética e as infraestruturas críticas nacionais". *Ciclo de Estudos Estratégicos* 10.

Castells, Manuel. 1999. *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*. Reino Unido: Wiley-Blackwell.

Cepik, Marco. 2003. *Espionagem e Democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência.* Rio de Janeiro: Editora FGV.

Costa Júnnior, Arnaldo. 2011. "A história da Agência Brasileira de Inteligência: A contra-inteligência organizacional" (tesis de maestria, Universidad de Brasília). http://bdm.unb.br/bitstream/10483/2307/1/2011_ArnaldoMonteiroCostaJunnior.pdf.

Dandolini Aparecida, Giovani de Paula y João Artur Souza. 2012. "Tecnologia da Informação e Comunicação e as atividades de inteligência". *Revista Ordem Pública* 5 (1): 119-136.

DCAF Backgrounder 2008. "Contemporary Challegens for the Intelligence Community Geneva Center for the Democratic Control of Armed Forces", http://www.dcaf.ch/publications/kms/series_backgrounders.cgm?lng=en&size269=20& page269=0.

Gagnon, Benoît. 2008. "Cyberwars and Cybercrimes". En *Technocrime: technology, crime and social control,* editado por Stéphane Leman Langlois, 46-65. Londres: Willan Publishing.

Gama Neto, Ricardo, y Gills Lopes. 2014. "Armas cibernéticas e Segurança Interna-cional". En *Segurança e Defesa Cibernética: da fronteira física aos muros virtuais,* editado por Medeiros Filho, Ferreira Neto y Gonzales. Recife: Editora UFPE.

Harding Luke, David Leigh. 2011. *Wikileaks: A Guerra de Julian Assange contra os Segredos do Estado*. Sao Paulo: Campinas.

Hare, Forrest. 2009. "Borders in Cyberspace: Can Sovereignty adapt to the challenges of Cyber Security?". En *The virtual battlefield: Perspectives on cyber Warfare,* editado por Christian Czosseck y Kenneth Geers. Estonia: Cryptology and Information Security.

Herman, Michael. 1996. *Intelligence Power in Peace and War*. Cambridge: Cambridge University Press.

Herz, John. 1951 *Political Realism and Political Idealism. A Study in Theories and Realities*. Chicago: The University of Chicago Press.

Jentlenson, Bruce W. 2010. *American Foreign Policy: The Dynamics of Choice in the 21st Century*. Nova Iorque: Norton & Company.

Kello, Lucas. 2012. *Cyber disorders: Rivalry & Conflict in a Global Information Age*. Cambridge: International Security Program/ Belfer Center for Science/ International Affairs, Harvard Kennedy School.

Kent, Sherman.1967. *Informações Estratégicas.* Rio de Janeiro: Bibliex.

Kshetri, Nir. 2014. "Cybersecurity and International Relations: The U.S engagement with China and Russia", http://web.isanet.org/Web/Conferences/FLACSO-ISA%20BuenosAires%202014/Archive/6f9b6b91-0f33-4956-89fc-f9a9cde89caf.pdf.

Kuehl, Daniel. 2009. "From Cyberspace to Cyberpower: Defining the Problem". En *Cyberpower and National Security,* editado por Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, 24-42. University of Nebraska Press.

Levy, Pierre. 1999. *Cibercultura.* São Paulo: Editora 34.

Libicki, Martin. 2009. *Cyberdeterrence and Cyberwar.* Santa Monica: Rand.

Libicki, Martin. 2012. "Cyberspace Is Not a Warfighting Domain". *I/S: A Journal of Law and Policy* 8 (2): 321-336.

Lojkine, Jean.1995. *A revolução informacional*. São Paulo: Cortez Editora.

Lopes, Gills. 2013. "Reflexos da digitalização da Guerra na política internacional do XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá" (tesis de Maestria, Universidade Federal de Pernambuco).

Machado, Jussara de Oliveira. 2010. "Inteligência e Ciberespaço: Desafios do Século XXI" (tesis de Maestria, Escola Superior do Ministério Público de Minas Gerais).

Miles, Anne Daugherty. 2016. *Intelligence Speding: In Brief*. Washigton, Dc: Library of Congress.

Minc, Alain, y Simon Nora. 1981. *The Computerization of Society.* Massachusetts: Mit

Press. Congressional Research Service Report.

Morgenthau, Hans. 1985. *Política entre las naciones. La lucha por el poder y por la paz*. Buenos Aires: Grupo Editor Latinoamericano.

Nye Joseph. 2010. *Cyberpower*. Harvard Kennedy School: Belfer Center for Science and International Affairs.

Nye, Joseph S. 2014. "The Information Revolution and Soft Power". *Current History* 113 (759): 19-22.

Sheldon, John. 2014. "Geopolitics and Cyber Power: Why Geography Still Matters?". *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy* 36 (5): 286-293.

Shulshy, Abram. 1992. *Silent warfare: understanding the world of intelligence.* Nueva York: Brassey's.

Sims, Jennifer. 1995. "What is intelligence? Information for decision makers". En *U.S intelligence at crossroads: agendas for reform*, editado por Roy Godson. Nueva York: Brassey's.

Sommer, P. Ian Brown. 2010. *Study: unlikely there Will ever be a pure "cyberwar"*. Inglaterra: University of Oxford.

Sun Tzu. 2007. *A arte da guerra: os treze capítulos originais.* São Paulo: Jardim dos Livros.

United States. The White House. 2011. "International Strategy for Operating in Cyberspace, Washington, Dc.

United Sates. 2009. "Cyberspace Policy Review", https://www.dhs.gov/sites/default/files/publications/Cyberspace_Policy_Review_final_0.pdf.

Ventre, Daniel. 2012. "Ciberguerra". Ponencia presentada *XIX Curso Internacional de Defensa*, Jaca, España, 26 de septiembre.

Vigevani, Tullo, Paulo Veiga y Karina Mariano. 1994. "Realismo versus globalismo nas relações internacionais". *Lua Nova* 34: 5-26.