Brazil´s cyberspace politics: Combining emerging threats with old intentions

Tiago Pedro Vales

tpvales@gmail.com

Tiago Pedro Vales (Brazil), graduated in International Relations by the University of the State of São Paulo (UNESP) and master in History and Political Culture at the same university. Advanced Studies in Peace and International Security at the University of Coimbra (Portugal). Current PhD Candidate in International Relations – International Politics and Conflict Resolution at the University of Coimbra, Portugal. Research interests includes Securitization and de-securitization processes, peace and conflict resolution, cyberspace policy and new emerging threats. The present work is part of a project funded by the Fundação para a Ciência e Tecnologia (FCT) in Portugal.

Abstract

The rise of the Information Age, mainly in the post-Cold War period brought a new dimension or elements to the safety and security for nationals and global agendas. Nowadays, relevant Information Technology and Internet Companies such as Google, Facebook, and Microsoft apace with International Organizations like World Telecommunication Union are implementing policies for the diffusion of this technology. They justify their practices with the argument of enabling social development and emancipation through providing access to information. The States and other International Organizations such as The North Atlantic Treaty Organization (NATO) and some private companies have been concerned with security issues on this theme. In this context, Brazil has drawn attention by implementing some measures to improve the governance of cyberspace, by legislating a law known as Marco Civil da Internet (Brazilian Civil Rights Framework for Internet). It was regulated in 2014 and included some participation in international forums defending an international commitment on this theme. In order to further understand how Brazil is developing its role on these issues, the main argument of this paper is that Brazilian policy has at least two sides. From one side it covers a raising security necessity and in the other, the security of cyberspace and internet provides an important field in international agenda where Brazil traditionally tries to improve its participation and relevance.

Keywords

Brazil, Foreign Policy, Cyber security, International Security.

Introduction

Nowadays, the Information Technologies has become a relevant part of daily life all over the world, mainly in the developed countries. From the early 90´s - with a new political background and a more open world economy - the Information Technologies became accessible by a large part of society. This facilitated the delivery and development of services in general, especially the technological and information based. These new tools and the spread of information contributed to the development of this same tools and, consequently, increased dependence among individuals, companies, governments, etc. From exchanging e-mails to rapid communication, from reading a newspaper to move large sums of money instantly around the globe, the Information Technologies (cellphones, pagers, computers, electronic devices in general) are not only present but essential. Connected and personified though the Internet, those technologies allowed a new virtual reality called cyberspace, which has the ability to define while is defined by the social reality, creating, as some authors argue, a new social paradigm based on the sharing information with no borders and no time limitations (Lévy, 2003; Castells, 2005).

Recently, big companies like Google have implemented measures to provide access to non-connected people, mainly from underdeveloped countries (Rushton, 2014), with the justification on the idea that providing access to cyberspace to these people is a tool for emancipation. On the other hand, countries and international organizations are worried about the security issues that cyberspace could provide. The North Atlantic Treaty Organization (NATO), for example, developed a National Cyber Security Framework Manual (NATO, 2012) and a Cooperative Cyber Defense Centre of Excellence, headquartered in Tallin, Estonia.

Among the discussions of providing access to Information Technologies, some episodes that concerned the world in terms of threats from the cyberspace, the security and defense measures to be taken, the cyberspace issues started an issue that gradually taken the center of the discussions on security worldwide. This is also an open opportunity for some countries to use the security discourse to claim better places or have their points discussed and drive multilateral decisions. This seems to be the case of Brazil in the recent initiative to advocating the creation of tools for the governance and security in cyberspace in international forums.

This papers aims to answer the question on what has led some countries, namely Brazil, to internationally defend the creation of measures for governance and security for cyberspace. The main argument is that the issue of cyberspace security is also an opportunity for Brazil to develop the traditional goals of its foreign policy. Apart from the security issue, driven by the episode involving the Brazil-US relations in a complaint of espionage, Brazil's role also serves its foreign policy issues that are also seen in other initiatives in leading discussions on emerging issues looking for a more relevant place in international community.

To develop this text, the first part discusses the theories of securitization in order to provide a theoretical framework to understand why and how the discourses are used in international forum to raise security worries and drive multilateral decisions. The second part is dedicated specifically to the Brazilian case in the cyberspace issue. It starts with a brief discussion of the principles and main aspects of the Brazilian foreign policy in the last decades. This summary is useful for to understand the Brazilian motivations in their multilateral actions. Following, there is an analysis of the Brazilian conduct on the very specific action of governance of cyberspace addressing its domestic motivations and international actions pursuing specific goals.

Cyberspace and the securitization theory. A possible debate?

The Cyberspace as an emerging security issue

In the post-Cold War, a new perception was developed, and the security issues once limited to local levels became relevant in internationally. It is possible to note that the notions of globalization dynamics on several issues such as economics, environment, civil conflicts, the responsibility of protection became a new paradigm for international security discussions and interventions. Internal elements has exceeded the bounds of State borders. Such particularities became a central argument to political discussions and decisions at different levels of governance and in academic issues (Novaes, 1992; Berdal, 1996; Black et al. 2006; Spillmann, 2000; Liotta & Owen, 2006). These themes challenged international politics and the role of the State in international relations (Tutuiani, 2013) offering opportunities to improve the definitions of security, that has incorporated themes not necessarily linked to traditional territorial-military issues.

The last changes in economy and policy, allied to technological development, have led to a post-industrial era. This new social paradigm is focused on social and production aspects based on a growing dependence on specific expertise. This new dimension of social structures is widely identified as the Information Society or Age of Information among other similar terms (Barney, 2004; Castells & Cardoso, 2005). According to Bell, the main characteristic of this post-industrial society is that sources of innovation are derived from the accumulation and dissemination of technical and theoretical knowledge, which makes contemporary society a true information society (Bell: 1976). From the 1990s on, this post-industrial scenario is identified with global information production and sharing knowledge. Based on electronic and digital data transmission at high speed and efficiency and at no cost or insignificant costs, the Information Technologies (ITs) have gained global importance, while they have become crucial to some important social necessities. More than that, the dependence on these new technologies, due to their ability to penetrate social use and distribution, is a practice to be encouraged, as predicted by the International Union for Telecommunications (ITU) (2003) which has a political endeavor to disseminate the use of IT as a tool to promote economic development, etc.

The quick diffusion of IT and the growing capacity of connection and transmission of information, constituted what some authors identify as a network society (Barney, 2004; Castells, 2005). According to Castells, this society is characterized by specific culture, institutions and private and contextual. This society´s culture shares some basic settings that characterize the current social model as a distinct form of human organization (Castells, 2005).

This society, in general terms, has improved itself and constituted a paradigm shift that, according to Castells (2005), would be the Paradigm of Information Technology. The author defines three characteristics for this paradigm: 1) information is taken as raw material, 2) high capacity of penetration of the effects of these technologies, since information involves all human processes. Individual and collective spheres are directly shaped by technological processes and 3) adaptation of the increasing complex of the interactions made within virtual networks. Castells (1999: 24-26) believes that these interactions made through virtual networks, allowed by the access to computers and the internet, created new forms and channels of communication in a mutual interaction. The author states that in a globally interdependent system, relations and exchanges are made and unmade according to goals processed in networks where strategic decisions are presented. In this context, the technological development, mainly in the Information Technologies, represents a major sector of the contemporary globalized and interdependent economy (Albert & Papp, 1997: ii)

Thus, it is seen that the evolution of IT enabled a new free from boundaries globalized public space, for now, without a complete control by any State or other entity. This space, in particular the internet and its tools is called cyberspace. This space has pervaded social relations allowing different actors to meet and develop their interests in a large and dynamic network of contacts and possibilities. According to Bells´ (2001) definition,

> Cyberspace is a term used to describe the space created through the confluence of electronic communications networks such as the Internet which enables computer mediated communication (CMC) between any number of people who may be geographically dispersed around the globe.

Among the challenges posed by the rising of cyberspace for International Relations lie the security issues in several areas: terrorism, theft of data, access control, and operation of infrastructure, hacking attacks, cyber warfare (Lewis, 2002). Evaluating such threats or challenges, States and multilateral organizations have taken certain measures or policies to promote cyber security threats as well as to prevent.

Just as it has brought benefits, the cyberspace and the development of the IT enabled the rising of new threats, from robbery to actions against critical infrastructures passing by the exploitation of internet by terrorist organizations. This perception put the cyberspace at the center of a debate about domestic and international security. The protection of cyberspace appears between the national security priorities in several countries and international institutions such United States and Australia, Atlantic Alliance and European Union (White House, 2013; Australian Government, 2009; European Commission, 2013; NATO, 2011).

Labeling security: a theoretical framework of securitization

The decision on what is a priority among the security issues is a complex process. This context involves a set of elements, evaluations, interests and choices that end up stablishing, by the proper actor, a determined policy or set of actions directed to a particular purpose. This goal is obviously linked to what was addressed understood as threat to a critical element for a determined society or country. This process of setting a priority in security issues for a determined is theoretically systematized as Securitization theories, by Copenhagen School and others that came after as critical and complementary.

As argues by scholars from Copenhagen School, before becoming a security priority, these initiatives or strategies passes through what Buzan et al. (1998: 25), call *securitizing move*: "a discourse that takes the form of presenting something as an existential threat to a referent object". That is the first step to a securitization process. It includes the conviction of determined audience about the necessity of implementing special ways to urgent situations (Taurec, 2006). In this case of cyberspace, the discourse has been made very often by public authorities and organizations in general, U.S President, Barack Obama, (White House, 2009) and the Indian former minister of Communication, Kapil Sibal, for instance (India Times, 2013; DNA India, 2013; IBN Live, 2013).

In general, the discourses or speech acts made by these authorities try to address the justifications of the use or implement special measures. These measures point to the protection of critical infrastructures, that is, those essential to the functioning of a country or to the ones that allow the basic supply of the needs of a particular society, namely the energy network and facilities, water and gas sources, and services like transportation, health and financial. It is easy to address that the higher the dependence of the infrastructure of information technology in various sectors, the greater their vulnerability to threats from cyberspace.

Nevertheless, before being understood as a matter of security, threats from cyberspace are so identified by a speech act. Or as Buzan et al. (1998) points, before became a security issue, there is a speech act that drives a determined element as threatened and passive to be an object of special security measures. This movement is identified by the mentioned actor as a securitization process.

The idea of securitization is based in a broader view of emerging security concept from the 1980s and widely applied after the end of the Cold War. In this sense, international and domestic security is no longer seen as a subject of military field, it is, in turn, an open topic that can involve different aspects or sectors, as argued by Buzan (1998: 27). Thus, in the case of securitization theory, as the security issues are firstly addressed by a speech act (by a securitizing actor, the one who points out a theme as a matter of security) (Balzacq, 2005: 172) directed to a determined audience (that could be regular citizens or the international community, etc.) the security and threats are social constructions, and not a pre-determined item:

> "Security is thus a self-referential practice, because it is in this practice that the issue becomes a security issue – not necessarily a real existential threat exists but because the issue is presented as such threat"
>
> […]
>
> "when a securitizing actor uses a rethoric of existential threat and thereby takes an issue out of what under those conditions is "normal politics", we have a case of securitization". (Buzan et al. 1998: 24)

The securitizing process has three main aspects. The first is the referent object, or the element (that could be anything) whose defense of their existence is legitimate provide justification for taking exceptional measures. The second is the securitizing actor, as explained above, the one who declare the referent object as threatened. Finally, the functional actor, is the one who are able to affect or influence the normal settings of rules of the security into a special situation, out of the normal practices.

The speech act plays a very important role in the securitization process. As Weaver addresses,

> "a designation of the threat as existential justifies the use of extraordinary measures to handle it. The evocation of security opens the way of the state [or the actor who are able to set this special measures] to take special power […]. As a result, ´security´ is the result os a move that takes politics beyond the stablished rules of the games and frames the issue as above normal politics" (Weaver, 2012)

Beyond that, the process of securitization is the speech act when the label of security is printed on a determined object or situation. This process is opened to everyone and everything. Theoretically, everyone who possesses the means and a proper discourse can securitize any issue or object. Of course, it depends on some important elements, such as a correct audience and the interests of those whose the discourse is directed and the entities or actors with the capacity to take the necessary measures.

Securitization as a theoretical framework for understanding the cyberspace as a raising security issue.

In this particular field of the securitization of cyberspace, Buzan et al. (1998), in "Security: a new Framework for Analysis", mention, in general terms, the raising of cyberspace as an future relevant issue to take into account to conflict analyses. Their references is limited to citations of Der Derian and Nierop works (apud. Buzan et al, 1998: 137; 163 - 164). Their ideas sustain the argument that despite the globalization processes that have eroded the state borders, there are dynamics still related and will continue linked to territorial and traditional security issues. However, the technological development and the growing dependence on these information technologies, by social sectors and infrastructures, constrained the legislation of security policies regarding cyberspace. These initiatives placed cyberspace on the focus decision and policymakers.

Buzan and Hensen (2009: 228) mention the cyberspace as a security element linking that to the international security context after the terrorist attacks of 9/11. The link terrorism-cyberspace became a security priority in many states. The authors state that the securitization of cyberspace happens through the perception of imminent threats and implies formulation of specific policies. Cyberspace is a securitized theme that permeates many security sectors and do not constitute a particular sector itself. Cyberspace presents elements that approximate to military worries and economic securities. There is a particular grammar used to identify the securitization of cyberspace.

This securitization aspect can be divided into three specific categories: 1) Hypersecuritization: the tendency to exaggerate the threats, beyond the hypothetic elements in any securitization process, which implies excessive measures; b) everyday security practices: identification of the risks or threats from cyberspace to everyday problems; c) technifications, basically the idea that the security might be a technical responsibility in charge of those who possess the knowledge. In other words, this sustains the idea that "if cyber security is so crucial it should not be left to amateurs" (Hensen & Nissembaum, 2009: 1167).

In that aspect, as pointed by Cavelty (2012), it is possible to verify a technic-military approach. The link between military issues and cyberspace security suggests a sense of urgency for security measures. At this point, the security of cyberspace is seen as a national security issue legitimating the development of measures different from the ones used to deal in economic and commercial fields (Cavelty, 2012: 142). This view is reinforced by the growing complexity of the hack attacks, for instance, a growing and sophisticated hacker activism or virtual espionage and specially the activities perpetrated by states, such as China. According to Ball (2011) China classifies cyberspace as a strategic domain and have made efforts to equate its cyberspace defense resources to United States ones.

Thus, the militarization of cyberspace is linked to securitization processes at least in two main ways: 1) The militarization comes with securitization processes: when there is a perception that the threats represent a national defense matter and 2) when the militarization of cyberspace means a development of technical dimensions in Hensen and Nissembaum (2009) terms, for instance as happens with US Army Cyber Command.

Hare (2010) also takes the military dimension as a securitization aspect of cyberspace. He elaborates an analysis model conjugating military aspects and social-cultural cohesion in order to classify the disposition of a country to securitize cyberspace. According to Hare, weak states (in terms of military power) with few socio-cultural cohesion are more likely to securitize cyberspace than strong states, i. e., with considerable military power and social-cultural coherent. However, Hare does not apply his model to any specific case.

The securitization theories concerning cyberspace is an emerging issue among the academic and politics forums. The authors concerned with this subject through this theoretical lens apparently didn´t achieve any consensus or a clear idea on what or how the securitization contributions could explain issues based on the security of cyberspace. It seems that every case has to be analyzed on their particular characteristics in order to first establish the theoretical bases still under construction.

Despite this, the securitization theories are useful to offer a theoretical framework complete enough to understand the behavior of some actors. The securitization theory also offers tools useful to understand some actions taken in multilateral environment concerning the mobilization of tools or creation of governance of cyberspace among other issues.

This seems to be the Brazilian situation while raising and sponsoring initiatives to provide governance and security tools for cyberspace activities. Beyond that, the role Brazil is playing also reflects, naturally, the old foreign policy intentions by this country. This will be better analyzed on the following section.

The securitization processes may not be complete or successful, but, as Weaver (1995: 50) argues, by identifying something as a security issue, something is done. The word ´security´ linked to something implies some urgent and special measures. The final goal of the securitizing actor depends on its interests and contexts, as pointed by Balzacq (2005). Thus, the use of security word involving determined issue, could become a strategy to turn the political discussion to other (desired by the actor) direction. This notion is useful to understand the dynamic of the interactions of decision makers and political representatives pursuing their respective interests in international or domestic levels. This situation seems to be the case of Brazil concerning the current cybersecurity policies. This issues will be exposed on the following pages.

Brazil using cyberspace to get more space

A brief resume of Brazilian foreign policy standards

Brazilian foreign policy and its institutions have been marked, in a general overview, by a stable and coherent approach to international issues. In the last years, the country has been looking forward to have its voice heard and considered at international level. Considering the period after 1985, when the government passed from the military to civilians and mainly after the foundation of the State with the Constitution in 1988, the country experimented a change at the priorities on its foreign affairs.

In a more open and democratic environment, the Foreign Relations Office, known by Itamaraty, set new priorities on foreign affairs an attempt of trying to reinsert the country in a raising world order. The main strategies were directed to reinforce the country actions at international institutions and a support or even sponsoring, multilateral initiatives such as Mercosul (South Common Market, Mercosur). Besides that, the new foreign affair´s initiatives invested in recover a more assertive role in multilateral forums centered in global issues, like the environmental and ecological discussions. The most visible example of this tendency is the country´s hosting of the United Nations Conference on Environment and Development (ECO-92) (Senado Federal, 2011).

The following period is marked by a foreign policy more active in international politics. The mandate of the president Fernando Henrique Cardoso is characterized by an intensification of the presidential diplomacy. Fernando Henrique Cardoso´s (1994 – 2002) academic profile and political trajectory contributed to this disposition of the country to assume new goals concerned in building a more protagonist role in international relations, focusing, meanwhile, in the adoption of the international regimes, regional integration and strengthening the Mercosul. At the end of Cardoso´s mandate, the Brazilian foreign policy was showing a State with a consolidated democracy, concerned and involved in global issues and supporting international institutions, International Rights, and trying to consolidate itself among the key countries in the international system. (Lampreia, 1998; Vigevani et al, 2003).

The election of a leftist president Luis Inácio Lula da Silva in 2002, came with a promise of change at the political and economic directions in force until then. These promised changes were never implemented, at least in the foreign policy principles. Instead, Lula strengthened the presidential diplomacy, managed dialogues with seemingly opposing forces, such as the World Social Forum, for example, and a strong presence of social base and permanent dialogues with key sectors of the world economy as the G8.

Lula has deepened the opportunities provided by the policies initiated by his predecessor. He involved the country in increasingly international ties and played actively in forums and multilateral policies, from regional issues like the political crisis in Honduras, for instance, to the Israel-Palestine conflict. At the regional level, he contributed in the creation of the South American Union of Nations (UNASUL) and the establishment and leadership of MINUSTAH. Besides that, the Lula´s foreign policy gave a relevant emphasis on cooperation between the developing countries, called South-South cooperation. Lula´s mandates are marked by the participation in international organizations with a particular agenda and the diversifications of partners, the actions in groups like BRICS, and at the center of global most important security issues such as the attempts of agreement concerning Iran´s nuclear production (Vigevani, 2007; Fonseca, 2010). Resuming, the Lula´s foreign policy reinforced the traditional principles of Brazil foreign policy and, at the same time, provided a prouder and active foreign policy diversifying the partners and fronts always searching for a more prominent place in international community (Almeida, 2004).

Different from Lula and Cardoso, the current president, the leftist from Lula´s political party Dilma Rousseff, in charge since 2010, gave preferences to Brazil´s domestic issues. The political and economic dilemmas forced Rousseff's administrations to solve internal problems with the endemic corruption, the inflation and recession threats and an ideological agenda presented that has been object of discussions. In spite of that, the president kept the international commitments and has been, in its way, active in international groups.

When the security of cyberspace meets Brazilian foreign actions

The Rousseff period, despite not being the most active period of Brazilian diplomacy, it at the center of discussions addressed in this paper. Cyberspace issues appear at this period with worries in two levels and Rousseff´s diplomacy saw an opportunity to raise the security and governance of cyberspace worldwide.

At the domestic level, some issues involving governing the cyberspace were already being discussed since 2009 with the Brazilian Civil Rights Framework for the Internet (in Portuguese, Marco Civil da Internet). This project, now approved by both Legislative Houses and sanctioned by Rousseff, established a legal framework, legal principles, guarantees and duties for individuals, companies and the State while using the digital network in Brazil. As the former ex-Minister of Justice classified: the ´Constitution of the Internet´. After many rounds and discussions at Parliament, the project became law in 2014.

This initiative has bases at the commitment signed in 2004 at the Organization of American States (OAS) when they established the Resolution AG/REG. 2004 (XXXIV-O704) titled "The-Inter-American Internal Strategy to Combat Treaties to Cyber Security" with the objective of create an Hemispheric warning and watch network concerning security in cyberspace (OAS, 2004). Its approval and sanction, however, was much more related to another international fact that pulled this project among the priorities of the government.

In 2013 some denounces involving espionage by United States, through its National Security Agency (NSA), reached the center of Brazilian government. According to the denounces brought to public by the former NSA employee, Edward Snowden, the agency spied on Rousseff and many other directors and executives from the high Brazilian bureaucracy causing serious diplomatic disagreements between both countries (Harding, 2014)[294]. The Brazilian press gave substantial emphasis to the case and pulled current discussions about the Civil Framework of the Internet favoring the approval, despite some objections from some civil sectors (Senado Federal, 2014).

Furthermore, it caused a diplomatic incident between United Stated and Brazil. Despite the diplomatic relations weren´t at its best moments, both countries kept very stable relations. However, in response President Rousseff canceled an official visit to Washington. In an official statement, the Itamaraty exposed that:

> "As práticas ilegais de interceptação das comunicações e dados de cidadãos, empresas e membros do governo brasileiro constituem fato grave, atentatório à soberania nacional e aos direitos individuais, e incompatível com a convivência democrática entre países amigos" (in Monteiro, 2013)[295]

[294] In fact, the acts of espionage wasn´t focused exclusively on Brazil, but had many countries targeted like France and Germany, for example.

[295] Illegal practices of interception of communications and data from citizens, companies and Brazilian government officials are serious issue and a threat to the national sovereignty and to individual rights, and inconsistent with the democratic coexistence between friendly countries. (Free translation)

This case also fueled Rousseff´s discourse at the 68th Section of General Assembly of United Nations. Pointing the severity of the acts of spying, Rousseff addressed that,

> "Estamos, senhor presidente, diante de um caso grave de violação dos direitos humanos e das liberdades civis; da invasão e captura de informações sigilosas relativas as atividades empresariais e, sobretudo, de desrespeito à soberania nacional do meu país.
>
> Fizemos saber ao governo norte-americano nosso protesto, exigindo explicações, desculpas e garantias de que tais procedimentos não se repetirão". (MRE, 2013)[296]

The denounces by Edward Snowden and the acts of spying by the US agency act ended up creating substances that served to promote and strengthen a speech anchored in the need to produce tools or policies to promote safety in cyberspace. This idea gained support form important leaders such as the German chancellor, Angela Merkel, who also had her electronic communications intercepted by NSA and the French president François Hollande (Matoso, 2014).

This discourse and initiatives seem to generate a result in favor of Brazil's performance. Following its foreign policy principles of developing tools at a multilateral level, Brazil - supported by Germany and other leaders - won the approval of the Resolution A/69/488 concerning the ´Right to Privacy in the digital age´. (AG, 2014).

Considering the acts and the discourses used by Brazilian decision-makers in international and multilateral forums, it seems that the country is taking every opportunity to reach a more protagonist role in international relations. In this issue of cyberspace and the raising an popularization of Information Technologies and despite the security measures that may drive the discussions, could be seen as a door for Brazil to get more involved in central discussions of international agenda, just like the other fronts Brazil is attempting a leadership, including the most important declared mains goal which is becoming a permanent member of United Nations Security Council in a possible reform of this organism.

Of course, there are more issues involved than a mere discourse in the case of promoting security of cyberspace. But even those questions reinforce the idea that the country is pursuing its old goal of becoming a relevant actor. To further clarify this argument, the former Ministry of Defense and former Ministry of Foreign Affairs, Celso Amorim, argued that despite the threats from cyberspace are something relatively new, it is becoming an important issue for the security of the States and, doing nothing is not an option because this can lead to a similar situation to what happened with the Non-Proliferation Treaty: "Se nada for feito, o risco que corremos, diante da escalada contínua de arsenais ofensivos [armamentos cibernéticos] é que, em algum momento, venha a ser proposto um tratado que congele as disparidades do poder militar cibernético"[297] (Amorim, 2013: 292).

This discourse reveals a double need and challenge for Brazilian foreign policy. Firstly, there is a will of becoming a world relevant country at the level of international institutions explored above. Also this leads to a security necessity dependent not only on the organization of the domestic

[296] "We are, Mr. President, faced with a serious case of violation of human rights and civil liberties; the invasion and capture sensitive information concerning the business activities and, above all, a disrespect for national sovereignty of my country. We made known our protest to US government, demanding explanations, apologies and assurances that such procedures will not be repeated. (Free Translation)

[297] If nothing is done, the risk we run, given the continued escalation of offensive arsenals [cyber weapons] is that, at some point, will be proposed a treaty to freeze disparities cyber military power. (Free translation)

security institutions but also on the performance of the Brazilian diplomacy. Both elements constitutes a challenge for Brazil for the next years. Resuming, new or possible security issues are important to Brazil not only because it may become a threat, but also because it can help the country to achieve the traditional goals of its foreign policy.

Final Words

The spread of Information Technologies and the easy access generated new worries on security and concerning about the core values of the democratic societies, such as freedom of speech and the right to privacy. Considering the positive effects and the permeation the Information Technologies achieved nowadays, it seems impossible to step backward. Turn off the networks or restrict the access is not an option, since some important sector of society, like economy, communication and finance and even military issues are now deeply dependents on the proper functioning of the technologies and networks for digital communication.

As the Information Technologies are becoming more important to society, actors in international system raise their concerns regarding the usage of these tools. This is the case of Brazil and other countries who found a good source to fuel the discourse concerning security in multilateral forum. However, security is not the only interest noted. The acts performed by Brasil, specifically, in the scope of international organizations are anchored in some traditional foreign policy goals.

A more active foreign policy is a Brazilian investment since the second half of 90´s and these practices become even more visible during the last decade. The discourse and the actions taken by Brazil at multilateral environments, are addressing cyberspace to a domestic demand, especially after the complaints of espionage by NSA. It also reflect a foreign policy position. In this particular case, by the way, the strategies of the country has achieved results, as it was possible to convince determined audience, namely some UN members, to approve official resolutions concerning policies for cyberspace.

Securitization theories are useful to understand the process by which countries could improve its discourse and achieve determined goals. These theories have been applied in many fields of security studies from the environmental issues to the spread of epidemic diseases. Every case has particularities and deserves to be taken separately and it seems to be the case of the cyberspace as well. Since cyberspace involve some new security issues that are taking an important place in the current discussions, the tendency of security studies must address the cyberspace as a new aspect bringing it to the center of theoretical studies in general.

This security issue of cyberspace constitutes a challenge to Brazil´s foreign policy. However, it seems difficult to assure this specific case it will be continued. Despite the fact that Itamaraty is a very independent foreign policy department concerned with State issues, in the last years, foreign policy has shown an increasing dependence on the presidential profile and action. The government has been sometimes more open to the international issues and occasionally focused on domestic issues. It seems that, if these new issues are dependent on a collaborative agenda, it also depends on the relations of the countries in a bilateral level. For example, it seems to be hard to build a cooperation network concerning the security of cyberspace without key actors like United States. In this case, espionage acts like the ones perpetrated by United States contribute to the spread of distrust among the nations making it difficult to reach any multilateral agreement.

It is also important to observe that the current domestic context in Brazil is very complicated. The president is facing an economic crisis which is causing the fall of the gross domestic product and the rise of an inflationary growth and unemployment rates. The president has also collected falls in her rates for approval before the population. Beyond that she has been politically isolated, which prevents her from taking effective measures to solve these internal problems. In short, Rousseff has been unable to provide efficient answers to the internal crises and this is the reason why the issues of foreign policy, including the ones related to cyberspace, tend to be deferred to a context where they can best address these issues.

References

Amorim, Celso (2013) "Segurança Internacional: Novos desafios para o Brasil". *Contexto Internacional.* 35(1) 287 – 311.

Almeida, Paulo Roberto (2004) "Uma política externa engajada: a diplomacia do governo Lula". *Revista Brasileira de Política Internacional*

AUSTRALIAN GOVERNMENT (2009) Cyber Security Strategy. Online. Disponível em: http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf. Acesso em: 10 de janeiro de 2014.

Balzacq, Thierry (2005) "Three faces of securitization", European Journal of International Relations June 2005 11(2) 171-201

Barney, Darin (2004) The network society. Cambridge: Polity

Bell, Daniel (1976) The coming of post-industrial society. New York: Basic Books

Berdal, Mats (1996) "The security council, peacekeeping and the internal conflict after the cold war". *Duke Journal of comparative & International Law,* 7(71)*, 71 – 91.*

Black, David (2006) *A decade of Human Security: What prospects for global governance and new multilateralism?* In Black, David et al. (2006) A Decade of Human Security: Global Governance and New Multilateralism. Hampshire: Ashgate Publishing Limited

Buzan, Barry et al. (1998) Security: a New framework for Analysis. Boulder: Lynne Rienner

Buzan, Berry; Hensen, Lene (2009) The evolution of international security studies". Cambridge: University of Cambridge Press

Castells, M. (2005) A Sociedade em rede. Lisboa: Fundação Calouste Gulbenkian

Cardoso, G (1998) "Para uma sociologia do cyberespaço: comunidades virtuais em português". Oeiras: Celta Editora.

CAVELTY, M. The militarisation of cyber security as a source of global tension. In: MÖCKLI, D. Strategic trends 2012: key developments in global affairs. Zurich: 28 Center for Security Studies (CSS), 2012. Disponível em: . Acesso em: 12 ago. 2012.

DNAIndia (2013) "You are only secure till you are attacked, says Kapil Sibal at the Cyber Security conference. 14 de outubro. Acesso em 22 de março de 2014. < http://www.dnaindia.com/scitech/report-you-are-only-secure-till-you-are-attacked-says-kapil-sibal-at-the-cyber-security-conference-1903457>

EUROPEAN COMISSION (2013) Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open Safe and Secure Cyberspace.

Harding, Luke (2914) Os ficheiros Snowden. Porto: Porto Editora

Hansen, Lene; Nissenbaum, Helen (2009) Digital Disaster, Cyber Security, and the Copenhagen School. International Studies Quarterly, 53, 1155–1175

Hare, Forrest (2010) The Cyber threat to national security: why can´t we agree? Conference on cyber conflict proceedings, 2010

India Times (2013) "Some nations indulging in cyber crime, says Kapil Sibal". 11 de dezembro. Página consultada em 22 de março de 2014.<http://articles.economictimes.indiatimes.com/2013-12-11/news/45080625_1_cyber-crime-lawlessness-internet-freedom>

IBN Live (2013) "India will have cyber security policy soon: Kapil Sabal. 27 de fevereiro. Página consultada em 22 de março de 2014. < http://ibnlive.in.com/news/india-will-have-cyber-security-policy-soon-kapil-sibal/375470-11.html>

ITU (2003) "Declaration of Principles: Building Information Society: a global challenge in the New Millenium". Disponível em: <https://www.itu.int/wsis/docs/geneva/official/dop.html>. Acesso em: 12 de abril de 2014.

Lampreia, Luis Felipe (1998) "A política externa do governo FHC: continuidade e renovação" *Revista Brasileira de Política Internacional,* 41(2), Available at: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73291998000200001. Access in 20 July 2015.

Lewis, James (2002) "Assessing the risk of cyber terrorism, cyber war and other cyber threats" Center for Strategic and International Studies. Disponível em: <http://www.steptoe.com/publications/231a.pdf> Acesso em: 12 de abril de 2014.

Liotta, P. H., & Owen, T. (2006). Why human security? *Whitehead Journal of Diplomacy & Internationall Relations*, 7(37).

Matoso, Filipe (2014) "Dilma e Merkel discutem segurança eletrônica em encontro no Alvorada". Available at: http://g1.globo.com/mundo/noticia/2014/06/dilma-e-merkel-discutem-seguranca-eletronica-em-encontro-no-alvorada.html. Access 15th July 2015.

Monteiro, Tânia (2013) "Dilma cancela viagem aos EUA" *O Estado de S. Paulo.* 17 de setembro de 2013. Availabe at: http://politica.estadao.com.br/noticias/geral,dilma-cancela-viagem-aos-eua,1075730. Access in 20th July 2015.

NATO (2011) Defending the networks: the NATO Policy on Cyberdefense. Online. Disponível em: http://www.nato.int/nato_static/assets/pdf/pdf_2011
_09/ 20111004_110914-policy-cyberdefence.pdf. Acesso em 10 de janeiro de 2014.

NATO (2012) National Cyber Security Framework Manual. Tallin: Nato Publications. Disponível em: < http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf> Acesso em 20 de janeiro de 2014.

Novaes, Washington (1992) "Eco-92: avanços e interrogações". *Estudos avançados. 6(15),* 79 – 93.

OAS (2004) "Adoption of a comprehensive Inter-American strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating culture of cybersecurity". AG/RES. 2004 (XXXIV-O/04). Available at: https://www.oas.org/en/sms/cicte/Documents/OAS_AG/AG-RES_2004_(XXXIV-O-04)_EN.pdf. Access in 15th July 2015.

Rushton, Katherine (2014) ´Google spending $1bn on internet in developing countries´. Finance. The Telegraph. Available at: http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/10870369/Google-spending-1bn-on-internet-in-developing-world.html. Access in 21st July 2015.

Senado Federal (2011) ´Estocolmo´72, Rio de Janeiro´92 e Johannesburgo´02: as três grandes conferencias ambientais internacionais. Núcleo de Estudos Informativos, Boletim Informativo n. 6. Available at: http://www12.senado.gov.br/publicacoes/estudos-legislativos/tipos-de-estudos/boletinslegislativos/boletim-no-6-de-2011-estocolmo72-rio-de-janeiro92-e-joanesburgo02-as-tres-grandes-conferencias-ambientais-internacionais. Access in 20th July 2015.

Senado Federal (2014) ´Aprovado no Senado, Marco Civil da Internet segue à sanção´. Available at: http://www12.senado.leg.br/noticias/materias/2014/04/22/aprovado-no-senado-marco-civil-da-internet-segue-a-sancao. Access in 20th July 2015.

Spillmann, Kurt; Wenger, Andreas (2000) Towards the 21st Century: Trends in Post-Cold War International Security Policy. Brussell: Peter Land Publishers

Taurec, Rita (2006) "Securitization theory and securitization studies". *Journal of International Relations and Development,* 9 (1), 53 – 61.

Tutuianu, Simona (2013) Redefining Sovereignity: From Post-Cold War to Post Westphalia. In Tutuianu, Simona (2013) Towards Global Justice: Sovereing in a Interdependent World. The Hague: Asser Press

Vigevani, Tullo; Cepaluni, Gabriel (2014) "A Política externa de Lula da Silva: A estratégia da autonomia pela diversificação". *Contexto Internacional.* 29(2), Available at: http://fes.org.br/brasilnomundo/wp-content/uploads/2014/06/pe-de-lula-da-silva-tullo.pdf. Access in 20th July 2015.

Vigevani, Tullo et al. (2003) "Política Externa no período FHC: a busca de autonomia pela integração". *Temopo Social,* 15(2), Available at: http://www.scielo.br/scielo.php?pid=S0103-20702003000200003&script=sci_arttext. Access 20th July 2015.

Weaver, Ole (2005) "Securitization and desecuritization". In Lipschutz, Ronnie (1995) On security. New York: Columbia

Weaver, Ole (2012) "Aberystwith, Paris and Copenhagen. "The Europeanness of new "schools" of security theory in an American Field". In Tickner, A & Blaney, D. (eds). Thinking International Relation Differently. New York: Routledge

White House (2009) Remarks by the President on securing our Nation´s Cyber Infrastructure. May, 2009. Online. Disponível em: http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure. Acesso em: 22 de março de 2014.

White House (2013) Cyber Security. Online. Disponível em: www.whitehouse.gov/issues/foreign-policy/cybersecurity. Acesso em 10 de janeiro de 2014.

White House (2013) Cyberspace Policy Review. Online. Disponível em: www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf. Acesso em: 10 de janeiro de 2014.