Austral: Brazilian Journal of Strategy & International Relations
e-ISSN 2238-6912 | ISSN 2238-6262| v.7, n.14, Jul./Dec. 2018 | p.209-232

THE GEOPOLITICS OF THE SOUTH AMERICAN CYBERNETIC SPACE: THE (NON) SHAPING OF SECURITY POLICIES AND CYBERNETIC DEFENSE?[1]

Selma Lúcia de Moura Gonzales[2]
Lucas Soares Portela[3]

Introduction

The so-called cyberspace is the environment where all shades of information, whether economic, social, political or military, whether classified or not, travels and connect themselves. Additionally, it is the space where agreements, purchases and sales, legal or illegal activities and varied manipulations of data or information are stablished.

In such a context, it is not possible to write about security and/or defense without linking these subjects to the cybernetic space and its complexity: the crimes, thefts, domains, controls and the power relations developed in such space, in other words, without paying attention to the geopolitics of the cybernetic space.

Frequently, the South American regional environment is being analyzed from several angles and themes by researchers of many countries of the region, especially in the context of the regional forums, as the Organization of the American States, when talking about a broader regionalization, or, yet, in the scope of the Union of the South American Nations (UNASUR), from the perspective of the South America continent. Diverse themes such as human rights, regional cooperation, strengthening of democracy, indigenous

1 This article was developed from a working paper presented in the 60 Meeting of the Brazilian Association of International Relations, from 25th to 28th July, in Belo Horizonte, MG.

2 Professor at the Escola Superior de Guerra – Brasilia. Phd in Geography by the University of São Paulo. E-mail: selmagonzales@esg.br.

3 Master in Military Science by the Escola de Comando e Estado-Maior do Exército. E-mail: lucas.portela@hotmail.com.

peoples, sustainable development, peace promotion, among many others, are part of the research agenda. Regarding the cyberspace specifically, there were initiatives in the OAS more recently in the late 1990s, and, at the beginning of the current decade, there was a more specific debate in UNASUR.

At the OAS, the initial concern was to fight cybercrime and the actions of the organization were linked to the Ministries of Justice of member countries. Furthermore, in the 2000s, after the 9/11 terrorist attack, the concern was to create an Inter-American comprehensive cyber security strategy focusing on crimes, attacks and terrorism.

In the sphere of UNASUR, the first movement in relation to cybernetic space took place in 2012, at the time of the formulation of a work plan by the South American Defense Council (CSD), which supported the creation of a working group to deliberate on the possibility of establishing regional policies and mechanisms to fight cybernetic or defense-related cyber threats (UNASUL 2012).

Although these regional forums present proposals to develop policies and strategies related to cyber security and cyber defense, each member country establishes its policies independently. Occasionally the definition of the concepts of security and defense regarding the cyberspace is not even similar between countries, as well as their policies and responsible bodies.

For that matter, the present article proposes to analyze the political projects and the structures aiming the cyber security and cyber defense subject in the Southern American space, employing as a case study three South American countries with the greater density of internauts - Argentina, Brazil and Colombia –, placing these policies in the context of two regional forums: the Organization of the American States (OAS) and the Union of the South American Nations (UNASUR), and, from the analysis of such policies, verify if there is a similarity and interlocution between them or if they are discordant and if it is possible to consider that it is occurring a geopolitical configuration of the cyberspace in the region that influences the conformation of regional power.

In order to develop this research, we mapped the key policies of cyber security and cyber defense from the data collected in primary sources, as laws, decrees, resolutions, declarations and minutes published in the regional forums and in the countries surveyed, as well as secondary sources through specialized bibliography.

We structured the present article in five parts. Initially, we will make a brief conceptual discussion on the geopolitics of cyberspace; subsequently, we will present some considerations on the cyberspace, security and defense;

next, we will show the initiatives regarding the cyberspace developed in the scope of the OAS and UNASUR; and the specificities of the cyberspace in the defense and security policies of Argentina, Brazil and Colombia. Finally, the article will pose some considerations on the geopolitics of the Southern American cyberspace, focusing on the positioning of such countries regarding the institutional structures, spheres of activity and cooperation policies.

The Geopolitics of the Cyberspace

Before considering the potential geopolitics of cyberspace in South America, it is necessary to make clear the theoretical perspective that we are assuming, as well as the adjective proposition of the concept of geopolitics for cybernetic space. In this sense, the first question posed is about the legitimacy of the use of a field of knowledge oriented, a priori, to the territorial space to refer to the virtual space.

From the ontological perspective of the "geopolitical" neologism created in 1899 by the State Theory professor at the University of Uppsala, Rudolf Kjellén, it would not be possible to link geopolitics and cybernetic space considering that original meaning of the concept addressed the study of the influence of the soil (geographical situation, space occupied and territorial domain, consubstantiated in its resources to be explored) on the political phenomena. In elaborating his theory, Kjellén conceived an essentially continental space, perhaps maritime, given his concern of the state territory being an organism connected to the soil and in constant struggle for more space.

However, when we study political phenomena, we necessarily analyze relations of power and, for that matter, the field of knowledge of geopolitics carries, in its essence, analysis of relations of power and space, that is to say, not only the state space, which is the founding statement of traditional geopolitics, as it is enlightened by Heriberto Carou (2002, 206).

> Spatial reflection on power relations *cannot be limited* - as in the case of traditional geopolitics - *to those between States; It would be forgot then the numerous movements that occur on the sidelines*; it would operate in a reductionist way limiting "the political" to "the state". Thus, although critical Geopolitics e-emphasizes the microscale analysis (which deals with the entire planet), as was the case in the traditional framework, this cannot mean the abandonment of other scales, at the risk of falling into a determinism geographical[4] (Carou 2002, 206, emphasis added, our translation).

4 La reflexión espacial sobre las relaciones de poder *no se puede limitar* ---como ocurría en la

For that matter, we consider that power relations perform in different scales and dimensions just as they are only understood in the spatial context, in other words, the power needs a space to exist, since it cannot operate or be exercised in the vacuum, considering also that the power is always relative. There is no power if there is no associated object, once it is always exercised in relation to something or someone.

If in Kjellén's concept of geopolitics political relations and space were implied, these two dimensions, therefore, need to be taken into account in contemporary geopolitical analysis: politics (power) and (geographic) space where it is exercised. In this sense, which spaces can be considered?

At the current scenario, new spaces present themselves as *locus* where power relations occur, as well as other actors, besides the State, participate in this game. In this way, the geopolitical analysis incorporates new spatial dimensions, other actors and diverse powers.

Thus, cybernetic space presents itself as another *locus* where power relations (political) happen. Could we consider it as another geographical space? What categories and constitutive elements does this "virtual space" exhibit so that it can be considered a geographic space?

According to Walfredo Ferreira Neto (2014, 79 - 85), the control of the virtual space is exercised by the most capable actors, despite being seen as a global and common space; due to this fact it becomes territorialized. The author goes on to say: "In the globe's cybernetic environment, States define their territories [...]. Immediate examples, but not the only ones, are the domains of the ".br", ".us", ".uk", ".it"; ..., which perfectly indicate their respective territories".

In the constitutive aspects of the cyberspace there are borders that, agreeing with Ferreira Neto (2014, 70), must be seen in the form of a point, which can be at the same time information in its "package", or a "knot" of a highway, or, still, a strategic structure or critical infrastructure selected as a result of the resources available to the State.

If we accept the existence of a cyberspace geography, then, it is possible to address cyber-geopolitics, with specific characteristics in each place, according to the actors involved and the policies that focus on it, as well as conflicts, crimes, policies and strategies elaborated with the intention of man-

---

Geopolítica tradicional - *a las existentes entre los Estados; olvidaría entonces los innumerables fIujos que ocurren al margen; operaría de forma reduccionista limitando «lo político» a «lo estatal»*. De este modo, aunque la Geopolítica crítica hace hincapié en la microescala de análisis (la que se ocupa del planeta entero), como era el caso en la tradicional, esto no puede significar el abandono de otras escalas, a riesgo de caer en un determinismo geográfico

age, protect, expand and attack it, that is to say, policies and power relations in and for cyberspace.

Cyberspace, Security and Defense: Some considerations

Throughout history, we found numerous examples of civilizations that valued the discourse and its study, for example, when Rome was an empire. The importance of this exercise was so significant for some civilizations that they have studied the discourse through oratory and rhetoric, as the Athenians did.

Through these studies, one could read not only the content, but also the interests and intentions of its author. Although a policy is not a discourse, in analyzing it we can understand values and interests of the agents of the political game (Serafim and Dias 2012). However, one may stress that we are addressing political analysis and not is evaluation.

Although both terms seem to be synonymous and both can be applied to policies, the focus and result generated are distinct (Serafim and Dias 2012). An evaluation consists in observing the consequences that a particular policy causes, verifying its efficacy in front of a given problem. In the case of the present article, we do not intend to look the results of the cyber defense policies of Argentina, Brazil and Colombia, yet, the interests, positions and interactions of such countries, in view of this, to analyze and not evaluate.

That said, a policy analysis should address three levels:

Table 1 - Levels of Policy Analysis

Level of analysis	Descrição
Institutional	Examine the interactions within the institution(s) involved. This level looks at the decision-making process within an organization, as well as the relations it maintains.
Decision making process	In this level the interests of the agents involved are studied, as well as their reaction towards internal and external stimuli.
State-Society Relation	Considers States' rules and institutions. Power relations within them and the interaction of these structures with society. This level connects the other two levels, revealing the interests behind the policies employed.

Source: Dagnino (2002).

Defense policies generally consider the international environment as a motivator; so, the policy analysis should include a level regarding the international context. This context should consider existing power relations, at the regional and global scopes, the country's position on the international scene, especially on some issues, as well as existing conflicts, summarizing, a geopolitical analysis of the international situation. This level gains more emphasis within the issue of cyberspace that presents cross-border characteristics.

In order to apply the proposed analysis at the beginning of the topic, we must first distinguish cyber defense and cyber security. The separation of these concepts can guide the analysis of the adopted policy. However, it is worth noting that this is an analytical exercise at the ontological level, since in cyberspace the concepts interconnect (Portela 2015).

As Paulo Carvalho (2011) states, cyber defense can be described as the set of actions performed in cyberspace, aiming at the defense of systems and information. Through such perspective, cyber defense presents value in the integrity of the force, especially in the production of knowledge and intelligence. It should be emphasized that this author includes not only defensive actions in cyber defense, but also exploratory and offensive actions.

In turn, cyber security is associated, by Oscar Medeiros Filho (2014), with the dimension of public security. For this author, cyber defense is connected with the notion of war, while the cyber security one is related to an illegal sphere. Therefore, in his view, the conceptualization of cyber security and cyber defense is connected with the threat that is being fought.

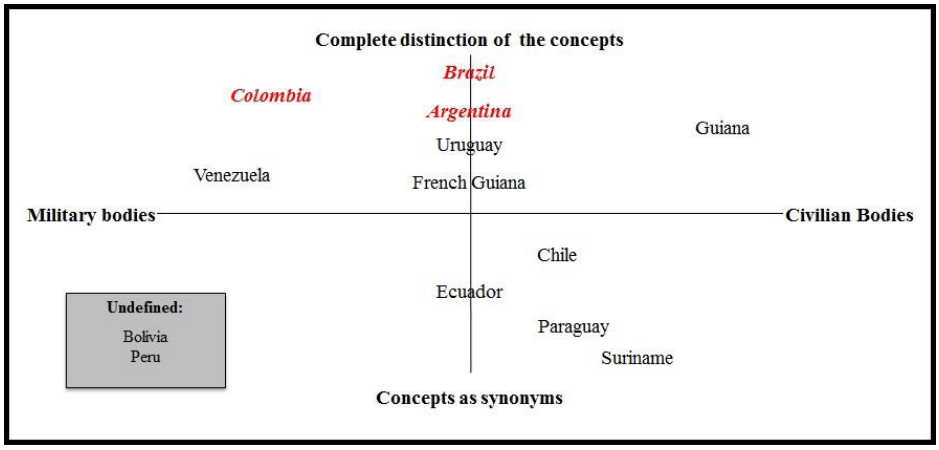
Moisés Naim (2006) addresses the question in a similar way when arguing about the limits of the concepts of traditional security and defense. About these concepts, Naim (2006) states that defense is related to war, defense of national interests, guarantee of survival and sovereignty, while public security is related to issues of illicit. So to distinguish cyber security and cyber defense we need to identify what cybercrimes are.

These can be categorized in two groups: cybercrimes and cyber-attacks (Portela 2015). In agreement to McGuire and Dowling (2013), the categorization of such concepts must be performed through the analogy and applicability in the traditional environment. For example, an online extortion is a cybercrime, while a data theft from a military base is considered a cyber-attack, since it is an act of espionage and warfare.

After presenting these conceptual distinctions, we can categorize the framework of cyber defense, in a general view, through a Cartesian plan in which the axis represent a gradual scale regarding the understanding of the distinction of the concepts of cyber defense and cyber security, while the other

presents the classification of the nature of the organization. In one extreme, we observe the structures that address the themes of cyber security and cyber defense with total separation and the other edge the structures that unite the themes, to the point of approaching them as synonyms. When we classify the institutions of South America in this plan, we find the following figure:

Figure 1 - Extract of South America Cyber Defense Structures (2016)



Source: Authors elaboration, based on Argentina (2010), Justribó et al (2014), Mandarino Jr. and Canongia (2010), Brazil (2012; 2013; 2015), Conpes (2011), Chile (2010; 2014), Paraguay (2013; 2015), Ecuador (2008; 2014), Uruguay (2005; 2014), France (2013; 2015) and Ministére de la Défense (2014; 2014b), Ministerio de Defensa (2015), Télam (2015), Contardo (2015), Velázquez (2015), Bonilla (2013), Infodefensa (2015) e IITCUP (2016).

Bolivia and Peru were categorized as undefined once there is no formal characterization, through documents and structures, that take into consideration cyber defense or cyber security. Argentina, Brazil and Colombia are highlighted in the figure above since they are the objects of this research; they present similarities for treating the concepts of cyber security and cyber defense in a different way.

The greatest divergence that we can observe in this group concerns specific structures for the treatment of cybercrimes. Colombia has only military structures, while Brazil and Argentina have hybrid foundation, with military and civilian organizations, dealing with cyber defense and cyber security respectively. The distinction between Argentina and Brazil is in the interac-

tion between the two scopes. Although Brazil has agencies that communicate between themselves, interaction is limited to mutual consultations.

Cyberspace within the regional forums

In the range of the American regional forums, we will present a brief overview of how the topic of cyberspace is treated in two of them: OAS and UNASUR. Although the proposal for the analysis is mainly the South America continent, it is important to situate the region in the context of a more hemispheric forum, in view of the double linkage of the South American countries with both organizations.

Cyberspace and the OAS

Within the agenda of OAS, the first initiative to approach themes related to cyberspace was the creation of a Group of Experts on Cyber Crime, discussed in the forum called "Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA)".

The goal of this group, comprised of government experts, was to perform diagnoses of illegal activities executed on computer networks, to identify national legislation, policies and practices relating to these activities and the national and international personalities experienced in the field, as well as to identify mechanisms for cooperation within the inter-American system to fight cybercrime (OEA / REMJA 1999)[5].

After the creation of REMJA's in 1999 the meetings of the Group of Experts on Cyber Crime, were held regularly, ranging from two to three years. The ninth and most recent one took place in 2016.

In order to facilitate and to make the cooperation and the exchange of information among the governmental cyber-experts of the OAS member

5 "Because of the importance and difficulty of the issues presented by cyber crime, and the spread and potential magnitude of the problems it poses for our countries, it is recommended to establish an intergovernmental expert group, within the framework of the OAS, with a mandate to:
1 - complete a diagnosis of criminal activity which targets computers and information, or which uses computers as the means of committing an offense;
2 - complete a diagnosis of national legislation, policies and practices regarding such activity;
3 - identify national and international entities with relevant expertise; and
4 - identify mechanisms of cooperation within the inter-American system to combat cyber crime" (OEA/ REMJA 1999, official translation)

states more efficient, an online portal[6] was created, in which the countries legislations on the subject, the recommendations from each Group of Experts meeting, and the proposition of a "24/7 High Technology Crime Contact Network" are listed, with the purpose to share and denounce cybercrime in international cooperation, involving other countries outside the OAS, such as the United Nations, the European Union, the Asia-Pacific Economic Cooperation Forum, the OECD, the G-8, the Commonwealth and INTERPOL. However, even though the propositions in this respect go back to the recommendations resulting from the meeting of the year 2000, at the 2016 meeting, those countries that had not yet adhered to that network were still oriented to do so in the shortest possible time.

> The objectives of the Group of Experts on Cyber Crime continue to be:
>
> > To strengthen the international cooperation in the investigation and prosecution of cybercrime, facilitate the exchange of information and experiences among its members and formulate the recommendations that are necessary to improve to improve and strengthen cooperation among the OAS member states and with other organizations or mechanisms. (OEA 2017, our translation)

However, in parallel with the existence of this Group, which focused only on cybercrime, in 2003 the AG/RES 1939 (XXXIII-O/03) "Development of an Inter-American Strategy to Fight Threats to Cybersecurity" was published, this resolution was approved at the fourth plenary session, on June 10, 2003.

In this resolution, it was recommended to the Permanent Council that a project on strategies of cybersecurity to the member States should be developed through the Committee on Hemispheric Security, in coordination and cooperation with the Inter-American Committee against Terrorism (CICTE), the Inter-American Telecommunications Commission (CITEL) and the Group of Experts on Cyber Crime of the Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA), or another body supported by the OAS. Therefore, a comprehensive strategy project was proposed, addressing the multidimensional and multidisciplinary aspects of cyber security (OEA 2003).

In 2004, through the adoption of the AG/RES. 2004 (XXXIV-O/04) by the General Assembly, the "Comprehensive inter-American cybersecurity strategy: A multidimensional and multidisciplinary approach to creating a culture of cybersecurity" was implemented and requested that the member

6 For more information on the online portal, check http://www.oas.org/juridico/spanish/cybersp.htm.

States of OAS implemented the guidelines contained in this document (OEA 2004).

Among these guidelines was the orientation for member countries to establish or to identify national "vigilance and alert" groups, the so-called Computer Security Incident Response Teams (CSIRT). Also, the creation of an Inter-American Surveillance and Warning for the quick dissemination of information on cyber security and the response to crisis, incidents and threats to computer security, as well as seeking to promote the development of a culture that would allow the strengthening of cybersecurity in the Hemisphere.

If on the one hand the creation of the Group of Experts on Cybercrime was conceived in the 1990s and focused on the creation of a network aimed at fighting cybercrime, on the other, the proposal to create a comprehensive cybersecurity strategy in 2003 was the result of the initiatives designed in a post-terrorist world of 9/11, in 2001. The concern in that moment was not only with crimes, but also with a strategy that involved cyber-terrorist threats, attacks on critical infrastructures[7], among other issues. It should be noted that the creation of the Group of Experts on Cyber Crime in 1999 did not mention the term "critical infrastructure".

Both the creation of the Group of Experts on Crime in 1999 and of the Comprehensive inter-American Cybersecurity Strategy, approved in 2004, failed to guarantee the effective participation of all OAS member countries. The recommendations contained in the IX Meeting of the Group of Experts on Cyber Crime, the most recent, urged member countries to comply with guidelines established by the group, six of which had not been accomplished by states yet, for example, the creation of a network: "the States that have not yet done so, in the shortest possible time, consider the possibility of joining the '24/7 High-Tech Crime Network' of the G-7". Regarding the Comprehensive Cybersecurity Strategy, from 34 (thirty four) member countries, only 17 (seventeen), that is to say, half of them presented Computer Emergency Response Teams (CERT) or Computer Security Incident Response Teams (CSIRT), bodies that the own OAS suggested as necessary and promoted their creations in the member States. From the 17 (seventeen) countries that have CERT or CSIRT, 11 (eleven) of them are members of the UNASUR: Argentina, Colombia, Bolivia, Brazil, Chile, Ecuador, Guyana, Paraguay, Peru, Suriname, Uruguay and Venezuela. The others are Canada, USA, Guatemala, Mexico, Panama, and Trinidad and Tobago.

7 We will develop a culture of cyber security in the Americas by adopting effective prevention measures to anticipate, address and respond to cyber attacks, regardless of their origin, by fighting cybernetic threats and cybercrime, typifying attacks against cyberspace, protecting critical infrastructure and securing the systems networks (OEA 2004, 129, our translation)

By analyzing the records and documents of the General Assembly of the OAS (qualified texts of Declarations and Resolutions), from the adoption of the comprehensive strategy in 2004, we could perceive that the issue of cyber security appeared to be linked to terrorism (2005 and 2011), to telecommunications (2006) and to strategies in the framework of the Caribbean Community/ CARICOM (2010, 2013, 2016).

We can infer that after the US government's spy scandal in Brazil, revealed in August 2013 by the former US Central Intelligence Agency (CIA) technical advisor, Edward Snowden, a movement emerged in 2012, in the context of UNASUR, for the creation of a working group on the theme, with a focus on cyber defense, an initiative that occurs in parallel with those existing in the OAS, weaking initiatives that more directly involved Brazil in this regional body.

Cyberspace and the UNASUR

The first evidence of UNASUR's concern with cyberspace issues was in 2012, when the South American Defense Council (CSD) formulated a work plan for that year. Among the points provided in the plan, UNASUR highlighted the need to create a working group to evaluate the possibility of establishing regional policies and mechanisms to fight cybernetic or information-based threats in the area of defense (UNASUR 2012). The leader of this group would be Peru.

In the following year, 2013, the work plan no longer required the assessment of the possibility of establishing policy, but rather its effective establishment, as well as regional mechanisms to fight cyber threats in the area of defense (Justribó 2014). It is noted, through these two documents, that UNASUR initiated its proposals of cyber defense distinguishing cybernetic threats of computer threats. Furthermore, these documents emphasize the fight of threats in the context of defense, that is, to distinguish this concept from that of cyber security.

That same year, the need for this organization to address cyber defense increased in the face of a real threat faced by Brazil in discovering cybernetic espionage by the United States, which was mentioned earlier. This event resulted in a special mention during the VII Ordinary Meeting of Heads of States in August, 2013.

> The South American Defense Council (CSD) and COSIPLAN instruct to evaluate cooperation with other relevant ministerial councils and to develop

> their respective projects on cyber defense and to improve the interconnection of our countries' fiber-optic networks with the intention of making our telecommunications safer, strengthen the development of regional technologies and promote digital inclusion (UNASUL 2013, our translation)[8].

Although there is no direct link with the Brazilian experience, the final declaration of this meeting reveals the urgency of promoting cooperation in cyberspace defense within UNASUR. In this case, the concern was not only the cooperation among the members of the organization, but it extended the proposition of collaboration to other regional organizations. It is possible to be seen that the securitization of the theme brought to the document of the VII meeting more concrete actions, such as the interconnection of fiber optic networks and the coordination of the CSD and the South American Infrastructure and Planning Council (COSIPLAN) to endorse a joint infrastructure (UNASUL 2013).

The August meeting that happened in Suriname was the initial point for the work in relation to cyber defense to become more concrete. In the working plan of 2014 it was provided the Regional Seminar on Cyber-defense (Justribó 2014). In this event, the Working Group on Cyber defense of de CSD identified the four topics below:

1. To create a regional forum of a Working Group on Cyber defense of the member States with the purpose of exchange knowledge, experience and solution procedures.

2. To establish a contact network of the competent authorities for the exchange of information and permanent collaboration

3. To define one platform and procedures of communication of the contact network

4. To deepen and systematize the thoughts of the conceptual definitions of cyber defense and cybersecurity (UNASUL 2014, our translation)[9]

8 Instruye al Consejo de Defensa Suramericano (CDS) y al COSIPLAN, evaluar la cooperación con otros consejos ministeriales competentes y avanzar en sus respectivos proyectos sobre defensa cibernética y la interconexión de las redes de fibra óptica de nuestros países, con el objetivo de tornar nuestras telecomunicaciones más seguras. Promover el desarrollo de tecnologías regionales y la inclusión digital. (UNASUL 2013).

9 1. Crear un foro regional del Grupo de Trabajo de Ciberdefensa de los Estados Miembros, a fin de intercambiar conocimientos, experiencias y procedimientos de solución. 2. Establecer una red de contactos de autoridades competentes para el intercambio de información y colaboración de manera permanente. 3. Definir la plataforma y procedimientos de comunicaciones de la red de contactos. 4. Profundizar y sistematizar la reflexión sobre definiciones conceptuales de

The result of this agenda was the creation of a network of contacts of the representatives of each country to deal with the matter, which would be communicated by electronic mail and telephony. The group also agreed on the need to create a coordination platform that would be called UNAC-ERT. Lastly, it was required that all the countries share their nomenclatures, concepts and terminologies of cyber defense and cybersecurity for a debate, compilation and conceptual standardization.

Even today, these demands and the new requests are part of the agenda of the Working Group on Cyber Defense of UNASUR. In the minutes of the I Virtual Meeting of the group of March 2017, the group listed six points of work that are still similar to the previous debates:

> - Situational diagnosis by country and/or region, which will establish the common starting point for the work of the group;
> - Contribution on the concept of cyber defense and cybersecurity;
> - Identification of institutions, terminologies and protocols that are used at the regional level;
> - Diagnosis on the context of regional threats, actors and motivations;
> - Definition of spaces for discussion and of proposals: forums, networks, platforms, observatories, etc.;
> - Proposal for Regional Policies and Strategies for cyber defense, which will be presented to the CSD-UNASUR for consideration and which will be raised to the highest level of the regional organization. (UNASUL 2017, our translation).

We notice that the measures and the progress of 2013 and 2014 were consequences of the momentary increasing of debates on cyber defense, which despite the results produced, did not meet the agenda of the time. Additionally, we note that the debate about the standardization of concepts and terms of cyber defense and cybersecurity is still an urgency to propose policies common to all members. Although we have not yet adequately addressed these issues, we note that UNASUR understands the two concepts distinctly, and also understands the need for standardization of cyber defense structures.

Cyberspace in the Defense and Security Policies of Argentina, Brazil and Colombia

There is no homogeneity in the South American cyberspace in terms

ciberdefensa y ciberseguridad (UNASUL 2014).

of institutional policies and structures, as well as in the approach to the concept of cybersecurity and the perspectives with which they are addressed[10]. Sometimes both cyber security and cyber defense are considered by a military defense structure, or in specific cases, there is one civil and another military structure.

In the framework of OAS, the policies and guidelines are structured with focus on cyber security and include two mechanisms: one that addresses the cybercrimes attached to the Department of Legal Cooperation of the Secretariat for Legal Affairs and the Meetings of Ministers of Justice or Other Ministers or Attorneys General of the Americas (REMJA) and another that addresses cyber security, the Integral Inter-American Strategy for fighting cyber security threats, attached to the Inter-American Committee against Terrorism (CICTE) and the Inter-American Telecommunications Commission (CITEL).

For that matter, the OAS focuses the cyberspace especially from a security perspective, and it seems to us that the organization's central concern is to maintain a structure to face cybercrimes and illegal activities, within the settings of terrorism, and not to use the terminology "cyber defense".

In the sphere of UNASUR, from what we have observed, the work focuses on cyber defense. The proposal, in 2012, to develop a Working Group had the intention to evaluate the possibility of establishing regional policies and mechanisms to combat cybernetic or defense-related information threats. Among the initiatives, a primary concern was the understanding and standardization of terminologies in the area of security and cybersecurity. Likewise, the execution of situational diagnoses in the member countries to identify the structural and institutional peculiarities in the cybernetic area to, subsequently, develop proposals of regional policies and strategies of cyber defense and present to the SADC-UNASUR.

Although the actions in this institution are incipient regarding cyberspace and are still at the level of diagnosis and standardization of terminologies, it is possible to affirm that the greater concern is the cyber defense, different from the initiatives within the scope of the OAS, which is focused on cyber security.

In relation to the three analyzed countries, Colombia addresses cyber-

10 Among the challenges which must be faced by the agenda of the South American Defense Council, in terms of cyber defense, are the different perceptions of the countries on the use of military and internal security resources. These conceptions on the use of the security and defense themes affect the different normative and doctrinal frameworks that rule the internal security and national defense systems among the member States of UNASUR, thus coherence in the confrontation of the questions regarding the cybersecurity and cyberdefense is difficult (Bustamante, Rivera and Cañas 2015, 112, our translation)

security and cyber defense in one particular sphere: the defense one, which can generate conceptual incompatibility when integrating a joint political strategy with other countries in the region. We believe that this fact is linked to the historical need to face local armed groups, seeking their disarticulation, as well as fighting cybercrimes.

In the Argentinian case, cyber defense is under the responsibility of the military structure, which also supports cybersecurity and it is linked to civil bodies.

In Brazil, the actions regarding cyber defense are under the responsibility of the Cyber Defense Command (CDCyber), subordinated to the Ministry of Defense, while aspects related to government cyber security are inside the structure of the Staff of Institutional Security, an executive power body, in addition to the existence of several private entities responsible for cyber security, through departments of information security or computing. These bodies cooperate with Brazilian cyber defense organizations.

Brazil and Argentina have similar agendas, essentially in terms of comprehensiveness, as their cyber defense agencies include several levels of strategic planning.

From the analysis performed, we do not notice among the three countries examined a power dispute or a cyber domain. Policies are more focused on internal issues and seek to meet the social, political and economic specificities of each country. On the other hand, there is still no effective convergence between these policies, which weakens the cooperation with consequences for the strengthening of the cyber defense and cyber security in the South American region.

Although these countries are part of two regional forums (OAS and UNASUR), the policies and initiatives in these forums seem to follow parallel scripts, with different approaches and purposes, not a conformation or convergence of guidelines and aspirations.

Regarding the cooperation between the analyzed countries, the actions are still in declaration stages and present as central characteristics the exchange of knowledge.

Argentina has shown its intention to cooperate in the cyber defense area in 2013. In Buenos Aires, during a meeting of the ministries of defense of Argentina and Brazil, Augustín Rossi and Celso Amorim endorsed a declaration on defense cooperation between the two countries. The declaration aimed to echo the need for bilateral integration to promote regional integration as a consolidator of a zone of peace (Brasil 2013).

The cyber defense was also approached in the declaration, mainly in a

beginning of bilateral cooperation between these countries for this matter, as follows bellow:

> They agreed on the need to promote cooperation in cyber defense and the creation of a bilateral subgroup of work on the subject. They also agreed to organize this year a visit to Brazil by the cyber defense authorities of Argentina to learn about the Cyber Defense Center of the Brazilian Army and they also welcomed the invitation that the Brazilian Minister of Defense made for Argentina to designate participants to the Cyber War Course for Officers (2014) and for Sub-officers (2015), in Brazil (Brazil 2013a, 02)[11]

The relation between Argentina and Brazil on cyber defense was initially designed as actions of mutual knowledge and confidence building between the two sides. They did not provide actions of joint institutions, but only visits and participation in courses. Therefore, we can state that the Buenos Aires Declaration on Defense of 2013 only allowed an approximation of the subject of cyber defense between the two countries.

This is evident when we observe the other actions provided by this declaration. The document can be divided into acknowledgments of ongoing or promoted works and predictions of future actions. In the other themes, the future actions required a deepening in the practical joint relationships that were already established, for example, the creation of Standards for Elaboration and Publication of Combined Doctrines between the two countries (Brasil 2013a).

In the following year, Argentina also signed a declaration that involved the cyber defense theme with Chile. Different from the one endorsed with Brazil, this one established joint and practical actions, with the creation of a Bilateral Group to deepen cooperation in emergency military assistance (Defensa Sur 2014). In addition, the declaration required the creation of a binational force that could be activated in emergency situations.

It is worth noting that far from attempting to increase military capabilities, Argentina uses defense agreements to get closer to other South American states. Bilateral dialogue, from this perspective, could serve as a basis for regional integration since it would promote peace in the region. However,

11 Coincidieron en la necesidad de impulsar la cooperación en defensa cibernética y creación de un subgrupo de trabajo bilateral en el tema. Acordaron además organizar durante este año una visita a Brasil de autoridades argentinas en ciberdefensa con fines de conocer el Centro de Defensa Cibernética del Ejército Brasileño y celebraron la invitación que el Ministro de Defensa de Brasil realizó para que Argentina designe participantes es el Curso de Guerra Cibernética para Oficiales (2014) y pará Suboficiales (2015), en Brasil (Brasil 2013a, 02).

such declarations still do not present a practical application in the area of cyber defense besides the exchanges of information and interaction between the human resources of the countries involved.

However, this policy had been reoriented nowadays. With the departure of Cristina Kirchner from government and the beginning of Mauricio Macri term, cyber-defense cooperation efforts are directed toward the United States. This is what gives foundation for the idea that defense cooperation is used by Argentina as a tool of government and not as a State project.

In 2017, for example, during the visit of the Argentine president to the United States, these governments announced the creation of a Bilateral Intergovernmental Working Group on Cybernetic Policy (Argentina 2017). The group should identify cybernetic vulnerabilities of mutual interest to both countries, as well as the development of joint initiatives. It is important to note that the announcement does not only involve cyber defense, but also cyber security.

Another difference of this working group regarding the declarations made in the South America scope is that besides boosting this matter among the two countries, it also requires cooperation in international forums relevant to the theme. This happens because these countries understand that space security depends on other international actors (Argentina 2017).

In the Brazilian case, cooperation in cyber defense presents the two directions, intraregional and extra regional articulations. In both cases, we can deduce that Brazil presents the same model of cooperation established in the above-mentioned cooperation with Argentina. Consequently, the country tries to emphasize bilaterally the importance of this space, creating subgroups of work on the subject and establishing mechanisms for the exchange of knowledge.

Added to Argentina, Brazil had already established these categories of cooperation with Chile, Germany and Mexico (Oliveira et al., 2017). In the case of Argentina, the subgroup of work has been meeting in order to deal with aspects of cyber defense (Brasil 2015a). Despite this, cooperation still persists in human resources, this time providing for internships in the area of cyber defense (Brasil 2015a).

Brazil's extra-regional cooperation in the area of cyber defense has increased with intraregional cooperation. In 2014, the country signed an agreement with Sweden. On that occasion, these countries made a commitment to assemble working meetings to deal with defense issues. The second working meeting took place in the following year in Stockholm. Between the first and the second edition of the cooperation meetings, these countries made several

exchanges of experiences on the subject of cyber defense. In the last stage of this cooperation, a Swedish delegation visited the Center for Cyber Defense of the Brazilian Army (CDCyber) (Soares 2016).

Still following the same path of knowledge exchange, Brazil signed an agreement with India in 2015. The plan to hold an international course of Strategic Studies in 2016 with the Army was foreseen: exchange of professors and researchers in cyber security and cyber defense and doctrinal courses in these two themes. More than a declaration of intentions, it is important to emphasize that the meeting with the Indians generated proposals agreed within the framework of the three singular forces,

Another category of international cooperation of Brazil in which cyber defense has been targeted are those related to natural disasters. In 2013, for example, the country signed an agreement with Spain on this subject. The theme of natural disasters was highlighted by the Spanish side as a matter of approximation with South American nations, which was received by the Brazilian side as an issue to be dealt with bilaterally (Brasil 2013b).

At the same meeting, the Spanish Minister of Defense Morenés revealed, likewise, the Spanish concern with matters inherent to cyber defense. The then Minister of Defense, Celso Amorim, described the Brazilian experience with CDCyber and proposed the exchange of information as the initial axis of cooperation (Brasil 2013b). Consequently, in general terms, Brazil works on cyber defense with other countries within the idea of knowledge exchange, especially regarding the Brazilian experience with CDCyber.

It is also important to mention the meeting between Brazil and Colombia in 2012. At that time, the countries agreed to create a Joint Commission to review the capabilities of their forces (El Tiempo 2012). Composed of military personnel, it would also evaluate the cyber defense of both countries (El Tiempo 2012).

Colombia presents a different profile from Brazil and Argentina regarding cooperation in cyber defense. Colombian cooperation is mainly at the multilateral level, especially in the OAS forum. Within this organization, Colombia received a mission that verified the situation of its cyberspace besides evaluating its capabilities in cyber defense (OEA 2014).

In the bilateral axis, Colombia established a cooperation with South Korea, which began in 2014. Unlike other agreements and declarations already examined, the subject of this cooperation is Information and Communication Technologies (ICTs). Besides emphasizing cyber security and e-government, this agreement still requires technology transfer (Mintic 2015). It should be stressed that Colombia deals with cyber security and cyber defense

in the same military sphere, so cooperation in cyber security has a direct impact on cyber defense.

Among the results of this cooperation is the Colombian electronic government portal, the electronic authentication system and the strengthening of technical capacities in response to cyber incidents and threats (Mintic 2015). Additionally, it has also led to the creation of a data storage center for the Colombian government, an advanced cybersecurity response course and a study of the strategic and operational model of the country's cyber security ecosystem (Mintic 2015).

In summary, agreements and declarations of cooperation in cyber defense are still in the early stages. Cooperation is addressed in the context of the exchange of knowledge and exchange of cyber defense agents, with the exception of Colombia, which has an agreement with South Korea with specific actions. Therefore, cybernetics is considered within a broad spectrum of national defense and is still used as a tool for approximation or as a political instrument.

Final Remarks

Cyberspace, differently from the State's one, exceeds borders and involves a global network that is shared worldwide. For that matter, in agreement with Madeiros Filho (2014), this environment demands new arrangements of global governance, among them is the discussion of an international regime to the discussion of this matter.

Although the cybernetic issue does not respect political borders, we noted that in the South American space it is still addressed primarily in the interior of the borders of the Nation States, as a domestic matter.

Through the analysis of documents, we observed that efforts have been made by OAS and by the South American Defense Council (SADC), two regional forums that the countries that were analyzed participate, in order to establish policies regarding cyberspace.

Some initiatives, such as the Action Plans of 2012 and 2013 (UNASUR), that proposed the creation of a Working Group to address the viability of establishing regional policies and mechanisms to fight cyber threats in the scope of defense, are examples; however, there is still no effectiveness in the policies promoted regarding the creation of regional convergence, although it has not been verified the rise of an old agenda in the power relations, having in the cyberspace the catalyst of possible obstacles that lead to litigation between States.

The three countries analyzed have a tendency to prioritize the national focus on their documents and this preference for domestic treatment is justified as the country needs to initially guarantee its national sovereignty. While they do not finalize the organization of cyber defense and cyber security on the national sphere, the South American countries try to acknowledge some guidelines of regional forums and seek some level of approximation through bilateral cooperation between countries.

It is important to stress a positive aspect in the policies analyzed regarding the cybernetic matter: they are relatively recent and are in the process of implementation, as well as their respective structures, which facilitates the debate on the deepening of the conformation and cooperation between countries.

To come to the point, this article sought to present a brief outline of the defense and security policies addressed to cyberspace in three countries of South America: Argentina, Brazil and Colombia and to place them within the framework of two regional forums (OAS and UNASUR). However, we did not intend to exhaust the matter, given its complexity and the need for further study.

REFERENCES

Argentina. Ministerio De Defensa. 2015. *Decisíon Administrativa 15/2015*. Buenos Aires: InfoLeg.

Bonilla, Javier. Centro de Ciberdefensa Militar en Uruguay. Defense.com. Seção Uruguay. Madrid, set. 2013. Accessed May 10, 2016. http://www.defensa.com/frontend/defensa/centro-ciberdefensa-militaru-ruguay-vn10000-vst342

Brasil. 2012. *Livro Branco de Defesa*. Brasília: Ministério da Defesa.

Brasil. 2013. *Política Nacional de Defesa*. Brasília: Ministério da Defesa.

Brasil. 2013a. *Declaración de Buenos Aires de los Ministros de Defensa del Brasil y Argentina*. Brasília: Ministério da Defesa. Accessed May 10, 2016. http://www.defesa.gov.br/arquivos/2013/mes09/comunicado.pdf.

Brasil. 2015. *Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018*. Brasília: GSI.

Bustamante, Gilberto Aranda, Jorge Riquelme Rivera and Sergio Salinas Cañas. 2015. "La ciberdefensa como parte de la agenda de integración sudamericana". *Línea Sur* 9. Revista de Política Exterior. Accessed May 10, 2016. http://sedici.unlp.edu.ar/bitstream/handle/10915/40184/

Documento_completo.pdf?sequence=1

Carou, Heriberto Cair . 2002. "El retomo de la geopolítica: nuevos y viejos conflictos bélicos". *Sociedad y Utopía. Revista de Ciencias Sociales*, n.19, Mayo. Madrid, España.

Carvalho, Paulo Sergio Melo de. 2011. "Conferência de Abertura: o setor cibernético nas forças armadas brasileiras". In *Desafios estratégicos para segurança e defesa cibernética*, organized by Otávio Santana Rêgo Barros. Brasília: Secretária de Assuntos Estratégicos da Presidência da República.

Chile. 2010. *Libro de la Defensa Nacional*. Santiago: Ministerio de Defensa Nacional.

Chile. 2014. Orden Ministerial nº 3.380. Estado Mayor Conjunto. Santiago: Ministério de Defensa Nacional.

Colômbia. Mintic. 2015. *Colombia y Corea desarrollan primera etapa del programa de cooperación em TIC*. Bogotá: Governo da Colômbia. Accessed Feb 12, 2018, http://www.mintic.gov.co/portal/604/w3-article-9541.html,

Conpes. 2011. "Lineamientos de Política para Ciberseguridad y Ciberdefensa." Documento 3701. Bogotá: Departamento Nacional de Planeación.

Contardo, Andrés Polloni . 2015. "Ciberseguridad: Estamos preparados". *Revista Escenários Actuales*, Ano 20, no. 1. Chile: CESIM.

Dagnino, Renato et al . 2002: *Gestão Estratégica da Inovação: metodologias para análise e implementação*. Taubaté: Ed. Cabral Universitária.

El Tiempo. "Colombia y Brasil profundizan cooperación en la frontera". Bogotá, jan. 2012. Accessed Feb 12, 2018. http://www.eltiempo.com/archivo/documento/CMS-10955537.

Equador. 2014. *Agenda Politica de la Defensa . 2014-2017*. Quito: Ministerio de Defensa Nacional.

Equador. 2008. *Agenda Nacional de Seguridad Interna y Externa*. Quito: Ministerio Coordinador de Seguridad Interna y Externa.

França. 2015. *French National Digital Security Strategy*. Paris: ANSSI.

França. 2013. *White Paper on Defence and National Security*. Paris: Ministére de la Défense.

Ferreira Neto, Walfredo Bento . 2014. "Territorializando o "novo" e reTerritorializando os Tradicionais: a Cibernética como espaço e recurso de poder." In *Segurança e Defesa Cibernética: da fronteira física aos muros virtuais*, organized by Oscar Mederios Filho, Walfredo B. Ferreira Neto and Selma Lúcia de Moura Gonzalez. Coleção I - Defesa e Fronteiras

Cibernéticas Pernambuco: Editora UFPE.

Gsi. 2017. *Missão do DSIC*. Brasília: DSIC. Accessed May 12, 2017. http://dsic.planalto.gov.br/missao-do-dsic

Iitcup. 2016. *Misión*. Bolívia: Academia Nacional de Polícias, 2016. Accessed May 12, 2017. http://www.iitcup.org/Mision.html.

Infodefensa. 2015. "Ecuador pone los ojos en los sistemas en ciberdefensa brasileños". *Infodefensa*. Quito, jun. 2015. Accessed May 12, 2017. http://www.infodefensa.com/latam/2015/06/10/noticia-ecuador-sistemas-ciberdefensa-brasilenos.html

Justribó, Candela . 2014. "Ciberdefensa: Uma visión desde la UNASUR". *VII Congreso del Instituto de Relaciones Internacionales*. Buenos Aires: UNLP.

Justribó, Candela, Sol Gastaldi, Sol and Jorge A. Fernández. 2014. "Las estrategias de ciberseguridad y ciberdefensa en Argentina: marco político-institucional y normativo". *Informe de Investigación*. Buenos Aires: Escuela de Defensa Nacional.

Mandarino JR., Raphael and Claudia Canongia. 2010. *Livro verde: segurança cibernética no Brasil*. Departamento de Segurança da Informação e Comunicações. Brasília: GSI.

Mcguire, Mike and Samantha Dowling. 2013. "Cyber crime: a review of the evidence". *Home Office Research Report* 75. Reino Unido: Londres.

Medeiros Filho, Oscar. 2014. "Em busca de ordem cibernética internacional". In *Segurança e Defesa Cibernética: da fronteira física aos muros virtuais*, organized by Oscar Mederios Filho, Walfredo B. Ferreira Neto and Selma Lúcia de Moura Gonzalez. Coleção I - Defesa e Fronteiras Cibernéticas Pernambuco: Editora UFPE.

Naím, Moisés. 2006. *Ilícito: o ataque da pirataria, da lavagem de dinheiro e o do tráfico à economia global*. Rio de Janeiro: Ed. Jorge Zahar.

OEA. ASAMBLEA GENERAL. 2003. *Actas y Documentos*. Volumen I. Trigésimo Tercer Período Ordinario de Sesiones. Santiago, Chile. Accessed May 12, 2017, http://www.oas.org/es/sla/docs/AG02290S12.pdf.

____. ASAMBLEA GENERAL. 2004. *Actas y Documentos*. Volumen I. Trigésimo Cuarto Período Ordinario de Sesiones. Quito, Ecuador. Accessed May 12, 2017, http://www.oas.org/es/sla/docs/ag02528s08.pdf

____. DEPARTAMENTO DE COOPERACIÓN JURÍDICA. 2007. *Portal Interamericano de Cooperación en materia de Delito Cibernético*. Accessed May 12, 2017, http://www.oas.org/juridico/spanish/cybersp.htm

____. 2014. *OAS Makes Public Recommendations on Cyber Security for Colom-*

bia. Estados Unidos: Press of OEA. Accessed Feb 12, 2018. http://www.oas.org/en/media_center/press_release.asp?sCodigo=E-196/14

____. 2017. "Portal Interamericano de Cooperación en materia de Delito Cibernético". Accessed May 12, 2017. http://www.oas.org/juridico/spanish/cybersp.htm

OEA. Novena Reunión del Grupo de Trabajo en Delito Cibernético. *Recomendaciones*. 12 y 13 de diciembre de 2016. Washington, D.C. Accessed May 12, 2017. http://www.oas.org/juridico/spanish/cybersp_expertos.htm

OEA. REMJA. *Recomendaciones II Reunion de Ministros de Justicia o de Ministros o Procuradores Generales de las Americas sobre Delito Cibernetico*. Lima, Perú - 1 al 3 de Marzo de 1999. Accessed May 12, 2017, http://www.oas.org/juridico/spanish/cybersp_reun.htm

Oliveira, Marcos Guedes de, Lucas S Portela, Walfredo Ferreira Neto, Adriana Marques, and Graciela Pagliari. 2017. *Guia de defesa cibernética na América do Sul*. Recife: Ed. UFPE.

Paraguai. 2015. *Decreto nº 3.275/2015*. Poder Executivo. Assunção: Ministerio de Defensa Nacional.

Paraguai. 2013. *Primer Libro Blanco de la Defensa*. Assunção: Ministerio de Defensa Nacional.

Portela, Lucas Soares. 2015. *Movimentos centrais e subjacentes no espaço cibernético do século XXI*. Dissertação (Mestrado em Ciências Militares, ECEME, 2015). Rio de Janeiro

Serafim, Milena Pavan and Rafael de Brito Dias. 2012. "Análise de Política: uma revisão da literatura". *Cadernos Gestão Social* 03, no. 01, jan-jun. Bahia: UFBA.

Soares, Fayga. "Brasil e Suécia realizam encontro bilateral na área de Defesa". *Ministério da Defesa*. Brasília, Fev. 2016. Accessed Fev 12, 2016, http://www.defesa.gov.br/noticias/18286-brasil-e-suecia-realizam-encontro-bilateral-na-area-de-defesa

Unasul. Conselho de Defesa Sul-Americano (CDS). 2012. *Acta da primera reunión para la conformación de un grupo de trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en ámbito de la defesa*. Lima.

_____. 2013. *VII Reunión ordinaria del Consejo de Jefas y Jefes de Estado y de Gobierno de la Unión de Naciones Suramericanas*. Paramaribo: UNASUL.

_____. Conselho de Defesa Sul-Americano (CDS). 2014. *X Reunión de la in-*

stancia ejecutiva del Consejo de Defensa Suramericano. Cartagena.

_____. Conselho de Defesa Sul-Americano (CDS). 2017. *Acta I Reunión Virtual Grupo de Trabajo Ciberdefensa CDS-UNASUR*. Equador: CDS.

Uruguai. 2014. *Política de Defensa Nacional*. Montevídeu: Ministerio de Defensa.

Uruguai. 2005. *Libro Blanco de la Defensa Nacional: aportes para um debate*. Montevídeu: Ministerio de Defensa Nacional.

Velázquez, Tomás. 2015. "Las Fuerzas Armadas paraguayas crean una unidad dedicada a la Guerra Electrónica". *Defensa.com*. Paraguai, abril. Accessed May 11, 2016. http://www.defensa.com/frontend/defensa/fuerzas-armadas-paraguayas-crean-unidad-dedicada-guerra-vn15398-vst335

ABSTRACT

The purpose of this article is to analyze the current cyber security and defense policies in Brazil, Argentina and Colombia, that have the higher density of internauts, placing these policies in the context of two regional forums: the Organization of American States (OAS) and the Union of South American Nations (UNASUR), and the possible existence of an interdependence among them or if a new cyberspace geopolitics is being framed in the region, that influences the organization of regional power.

KEYWORDS

Cyberspace; Geopolitics; South America.

Translated by Helena dos Anjos Xavier