ARTICLE DOI 10.22491/cmm.a003

An analysis of the cyberspace securitization process*

Un análisis sobre el proceso de titulización del ciberespacio

Abstract: Cyberspace manifests itself as a new domain for power relations as different actors use it to pursue their interests. Because it is endowed with a deterritorializing logic - in which multiple entities can act anonymously - cyberspace defies traditional conceptions of national security and defense, as digital flows cross different territories. Considering the insertion of the basic state infrastructure in the cyber domain, encompassing banking, telecommunications, transport and military systems, there is a growing dependence of society on cyberspace. Such dependency can be exploited by a myriad of international actors. In this context, through the conception of the Copenhagen School regarding the process of recognition of threats by securitizing agents, this article investigates the process of securitization of cyberspace by analyzing the white defense books of Brazil, Germany and France.

Keywords: Cyberspace. Safety. Defense. Territory. Threats.

Resumen: El ciberespacio se manifiesta como nuevo dominio para las relaciones de poder en la medida que distintos actores lo utilizan para perseguir sus intereses. Por ser dotado de una lógica de desterritorialización (pérdida de territorio) – en la cual múltiples órganos pueden actuar de manera anónima –, el ciberespacio desafía concepciones tradicionales de seguridad y defensa nacional, mientras que flujos digitales cruzan distintos territorios. Es considerada la inserción de la infraestructura básica de un Estado en el dominio cibernético, englobando sistemas bancarios, de telecomunicaciones, transportes y diversos agentes, como los militares, se observa una creciente dependencia de la sociedad con respecto al ciberespacio. Tal dependencia puede ser explotada por una miríada de actores internacionales. En ese contexto, por intermedio de la concepción de la Escuela de Copenhague con respecto del proceso de reconocimiento de amenazas por agentes de titulización, el presente artículo investiga el proceso de titulización del ciberespacio mediante análisis de los libros blancos de defensa de Brasil, Alemania y Francia.

Palabras Clave: Ciberespacio. Seguridad. Defensa. Territorio. Amenazas.

Breno Pauli Medeiros
Exército Brasileiro. Escola de Comando e Estado-Maior do Exército, Instituto Meira Mattos.
Rio de Janeiro, RJ, Brasil.
breno.pauli@gmail.com

Alessandra Cordeiro Carvalho
Exército Brasileiro. Escola de Comando e Estado-Maior do Exército, Instituto Meira Mattos.
Rio de Janeiro, RJ, Brasil.
alessandraccarvalho27@hotmail.com

Luiz Rogério Franco Goldoni
Exército Brasileiro. Escola de Comando e Estado-Maior do Exército, Instituto Meira Mattos.
Rio de Janeiro, RJ, Brasil.
luizrfgoldoni@gmail.com

Received: Dec. 13, 2018
Accepted: Jan. 24, 2019

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

* This paper is part of the research project "Science, Technology and Innovation in Defense: Cybernetics and National Defense" approved by Tender Notice 27/2018, Programa de Apoio ao Ensino e à Pesquisa Científica e Tecnológica em Defesa Nacional – PRÓ-DEFESA IV

1 Introduction

Cyberspace represents a new domain of power relations. Being partly dissociated from physical space, cyberspace has a logic of its own in which the traditional conception of borders hardly prevents the flow of information. As a new operating environment, cyberspace integrates private, military, civil and state actions into the technical-scientific-information environment. While cyberspace is consolidated as an alternative domain for the exercise of power relations, its logic and peculiarities pose challenges to traditional domains.

Shrinking physical distances, instantaneous communication and society's greater interdependence in relation to cyberspace raise questions on how to address defense and strategy in this new domain. Prominent among them are issues of securitization and the nature of potential "new" threats.

In this new environment – marked by more flexible borders and territories and multiple, anonymous actors – new and old threats challenge traditional conceptions of national security and defense. The frequency of cyber occurrences worldwide is well known. Malware,[1] ransomware[2] and DDoS[3] attacks, among others, besides expanding the number of possible aggressors to non-state actors, have become increasingly sophisticated, making it difficult to identify the authors or motivations behind them. Given this scenario of insecurity, cyberspace may be interpreted as a domain for the exercise of power, alongside the domains of land, sea, air and space.

The goal of this research is to investigate the process of cyberspace securitization in Brazil, Germany and France by means of a comparative analysis of their respective Defense White Papers. Studying the defense papers of the selected countries makes it possible to highlight the threats, strategies and practices that compose the cyberspace securitization process of states that have been targeted by cyberspace espionage and monitoring (BRIDI; GREENWALD, 2013; WIKILEAKS, 2015).

Due to limitations, this study will analyze the documents *White Paper on German Security Policy and the Future of the Bundeswehr*, *French White Paper: Defense and National Security* and *White Paper on Brazilian National Defense*, the latter together with its most recent version, the 2016 draft. The analysis was limited to the countries' Defense White Papers, since they represent the highest level of defense documents, setting the tone and approach of the documents that follow them hierarchically.

The content analysis of said documents shall be guided by four main questions: i) Does the document include a clear definition of cyber security?; ii) What does the document say about the cyber sector?; iii) What threats are considered?; and iv) What is the stance regarding

1 The most common types of malware or malicious software are viruses or worms, which have the ability to cause damage and self-replicate in computer networks and systems (GOLDANI, 2005).

2 A lucrative kind of malware that renders data stored in computers inaccessible through encryption, requiring users to pay ransom to retrieve them (SYMANTEC, 2016).

3 An attack technique involving a large number of computers – of which the owner may or not be aware – which overloads websites or servers by sending repeated service requests, making the system inaccessible (CARREIRO, 2012).

the involvement of other civil sectors? The study will also perform a comparative analysis of the defense white papers regarding aspects that deal with new and traditional threats related to the cyber issue and key terms that contribute to the understanding of the relevance of the proposed subjects. This will be done by creating comparative tables and word clouds that express the tone and the most prominent terms in each document.

With the insertion of today's society in cyberspace, actors use it to project power and interests. The deterritorialization character inherent in the cyber domain enables, for example, terrorist groups to recruit dissidents; intelligence agencies to monitor communications; and social movement activists to coordinate their demonstrations.

Cyberspace basically emerges as an alternative space in parallel with the traditional domains of land, air and sea; however, cyberspace has no borders, airspace or territorial waters (HILDEBRANDT, 2013). Operating in cyberspace requires no armored vehicles, jet fighters or battleships, just internet access. Thus, the spread of power inherent in cyberspace provides private actors with an operational domain in parallel with state forces (NYE, 2012). Cyberspace therefore takes on a strategic value for states and may also represent a new environment for non-state threats.

The increasing relevance of cybernetics in the context of security and defense justifies this study's goal of analyzing the process of cyberspace securitization as a strategic domain by regional powers. However, prior to the analysis of this process in Brazil, Germany and France, a few concepts and definitions should be presented to better contextualize the subject.

2 **Cyberspace: contextualization, concepts and definitions**

Cyberspace has various definitions – some more comprehensive than others – which contribute to the existence of a wide spectrum of approaches and understandings (KUEHL, 2009). Some consider it from a more theoretical viewpoint as a new area of interaction that pervades and interconnects telecommunications into a large global network, while others consider the physical and malleable aspects of the different connections and interconnected devices.

Lobato and Kenkel (2015, p. 24-25) understand cyberspace broadly as "the worldwide interconnected information networks and communications infrastructure that spans the Internet, telecommunications networks, computer systems and the information they contain." This definition proposes a broad approach to the concept of cyberspace as a large network of interconnected communications involving several actors connected to it.

Libicki (2009) offers a more specific definition, interpreting cyberspace as a less tangible medium than the traditional domains of land, air and sea. For the author, cyberspace is composed of three interconnected layers. The first is represented by hardware, physical electronic components such as cables, antennas and all kinds of interconnected devices, from computers and cell phones to armament systems, unmanned aerial vehicles (UAV) and so on. The second – or syntactic – layer consists of software. This contains the instructions and commands that developers and engineers give to the elements of the first layer so they may serve their purpose and communicate with each other. Last comes the semantic layer containing information in the form of binary data to be organized into lines of code or any other type of information.

In this context, cyberspace can be understood as a domain whose existence depends on the interconnectivity of information flows, in which are inserted all kinds of essential networks and infrastructure for today's society. Therefore, cybernetic space becomes a reality from the moment one or more devices are connected, serving as a platform for various human relationships. Because it includes different actors, cyberspace is a stage for unprecedented power relations. The latter generate different threats that interact, modify and exploit the information flows of the cyber domain.

In analyzing cyberspace, special attention should be given to three essential elements that represent peculiarities inherent in cyberspace and impose theoretical and practical challenges on social relationships. The first element is deterritorialization. Considering the physical elements of the hardware layer as devices that act in a similar way to knots in a large network of global communications, made up of information flows, such information flows are understood as corresponding to a reticular logic particular to cyberspace that interlinks the different physical devices interconnected by cyberspace. It is noteworthy that the traditional definitions and interpretations of territory understand it as the geographical area delimited by borders, corresponding to a spatially-based zonal logic, in which the state exercises sovereign control of the territory.[4]

The deterritorialization of cyberspace is present from the moment its reticular logic, in the form of interconnected flows, permeates the territory of different states; or when devices serving as nodes in the cyberspace network are controlled and/or exploited by other states. In other words, the interconnectivity of different points in a global network ends up permeating[5] the boundaries, considered essential to the zonal logic on which the concept of territory is based.

The second element corresponds to the diffusion of power in cyberspace. As the cyber domain emerges as an alternative space for the exercise of power, the diversity of actors in the network, together with easy access and acquisition of equipment and means, enable a relative reduction in the differences of capability between militarily stronger states, fragile states, non-state organizations and/or individuals. In this context, the number of potential threats grows exponentially, since new players use cyberspace for both soft and hard power (NYE, 2012). Indeed, Marcos Guedes de Oliveira (2014), in addressing the untapped potential of cyberwarfare, warns of the possible consequences of the actions of individuals in cyberspace that may affect systems on which society depends. According to the author:

> A brand new field of action is related to the facilitation of insurrections, demonstrations and even coups through the use and manipulation of resources shared via cell phone networks. Success in operations in this format would greatly reduce the costs of open and military intervention in smaller countries and give nations that dominate this

4 The concept of reticular and zonal logic is based on the analysis of network territory conceived by Haesbaert (2007), in which the different territorialities of groups and individuals merge with the territorial hegemony of states. The approach used here, however, uses the term in a sense more specific to cyberspace, considering the reticular logic of information flows within the cyberspace network that permeates the boundaries of the zonal conception of state territories.

5 This is a generalization. It is well known that countries such as China and North Korea have extensive restrictions on the use of their telecommunications and access to the global computer network.

> technology a strong argument in favor of non-regulation of the cyber environment at international level (OLIVEIRA, 2014, p. 194-195, our translation).

The third particularity stems from the uncertainty that develops in the cyber domain. Kallberg and Cook (2017), in addressing the challenges of cyberspace for traditional military thought, point out that anonymity and the difficulty to gauge the impact of a cyberattack are elements that contribute to the prevalence of the uncertainty principle inherent in cyberspace. Given its interconnected and highly complex nature, a possible attack can hardly be quantified or measured, since the effects are not necessarily kinetic and/or immediate, and are often concealed beneath numerous layers of semantic and syntactic networks.

Anonymity, in turn, can be used as a tool of both protection and attack. This can result in an incorrect identification of a cyberattack, leading to a possible counter-attack against innocent people and an uncontrolled escalation of the conflict. The emergence of the new domain raises to a new level the notions of "defeating the enemy without fighting" and "having others fight your battles."

The combination of deterritorialization, diffusion of power and uncertainty enables new and old threats to act in cyberspace within a scope ranging from diplomacy to sabotage, espionage, monitoring and even attacks with kinetic effects. Cyberspace is thus established as a stage for all kinds of actors and threats.

As an example, in 2013, Edward Snowden – a National Security Agency (NSA) analyst at the time – together with journalists from different countries revealed the NSA's spying and monitoring program. Countries such as Brazil, Germany and France had heads of state, government officials and companies monitored by the US agency, with the help of allied countries belonging to the so-called "Five Eyes," composed of security agencies of the US, Canada, Australia, New Zealand and the UK, which worked together to monitor citizens around the world (BRIDI; GREENWALD, 2013; WIKILEAKS, 2015; PRIVACY INTERNATIONAL, 2015).

Celso Amorim (2013, p. 289, our translation), prompted by spying in Brazil, spoke pertinently about the ever-finer line separating online espionage and cyberwarfare due to features such as uncertainty in cyberspace:

> Data monitoring and cyberwarfare share the use of very high-tech tools for activities that result in serious breaches of sovereignty. When the purpose of monitoring goes beyond mere observation and aims at obtaining technological knowledge, the boundary between espionage and war becomes increasingly harder to define. Conceptually, there would be no difference, except perhaps with regard to immediate damage, between an act of espionage, of search for economic and technological information, and a traditional attack to obtain an economic resource.
>
> Monitoring and cyberwarfare can target both countries perceived as hostile or representing immediate threats and friendly and allied countries. We already know that was the case in the data interception. We cannot exclude the same occurring with cyberattacks from any quarter. These two activities illustrate very clearly some of the new challenges of international security.

The monitoring exposed by Snowden is the exception to the rule, since the multiplicity of actors and anonymity in cyberspace makes the performance of national actors unlikely to be identified. However, it is possible to glimpse the performance of state actors in cyberspace, without confirmation or official recognition.

Perhaps one of the most emblematic examples is the Stuxnet case. This is a malware that contaminated the computers of Iranian nuclear centrifuges, sabotaging the country's nuclear project. All signs point to a cyberattack by the United States and Israel to delay that country's nuclear program. However, neither the Americans nor the Israelis ever actually accepted responsibility for the attack (KENNEY, 2015).

Monitoring or cyber sabotage carried out by other states constitute "old threats" in the sense that there has always been espionage, sabotage and wars between countries. However, they become "old threats" in cyberspace from the moment the diffusion of power forces them to act in parallel with other agents.

The new threats of cyberspace include not only those posed by states for the purposes mentioned above, but also threats by non-state actors. In other words, threats have crossed over from state level to the level of individuals. The latter have become capable, for example, of destabilizing governments by carrying out attacks with varied motivations. Non-state threats include cyber activism, cybercrime and cyberterrorism.

Cyber activism is defined as a cross of hacker action and political activism aimed at incapacitating servers or online websites (CEPIK; CANABARRO; BORNE, 2014). It can also be said that cyber activism is involved in issues related to certain causes, launching attacks against governments and companies that oppose their ideals to make them reassess their institutional decisions, thus drawing public attention to the defended cause (ZUCCARO, 2012).

Defined as an act or omission committed in violation of a law in cyberspace, cybercrime is a criminal activity related to illegal computer invasion, manipulation of information, sabotage of equipment and data theft (SAINI; RAO; PANDA, 2012). More broadly, it can be said that cybercrime is the development of illegal actions to be used in computer systems and networks. Using cyber espionage to test configurations and defense systems in order to gain access to sensitive information, cybercriminals can carry out cyber sabotage by generating obstacles by electronic means (CEPIK; CANABARRO; BORNE, 2014).

Despite not having a widely accepted definition – given the multiple meanings attributed to the word terrorism – (CHEN, 2014) cyberterrorism is generally interpreted as actions carried out by non-state actors against computer networks and systems, capable of resulting in violence against civilians. In addition, the attacks must have a political motivation and generate physical besides virtual damage (POLLIT, 1998; WEIMANN, 2005; KENNEY, 2015). According to Dorothy Denning (2000), cyber threats against computers, networks and systems aim to intimidate governments and populations in order to achieve social and political goals of groups and individuals. In addition, like the traditional form, cyberterrorism aims at widespread exposure and publicity (COLLIN, 1997).

Regardless of the motivation behind specific threats, cyberspace is revealed to be an environment in which different actions are carried out with variable levels of success. While bringing people together and allowing a range of previously unimaginable activities and services,

interconnectivity also opens doors to threats that were unthinkable in the recent past. Therefore, several states now recognize the importance of national cyber security and defense, since such attacks can generate irremediable physical, political, economic and social damage.

3 Cyberspace securitization

The post-Cold War global scenario led to the debate of new issues on the international agenda that became increasingly relevant in the 1990s, requiring the introduction of new models of security analysis (FARRET, 2014). Due to the inadequate theoretical-epistemological debate at the time, the analyses, previously focused on state-centered issues, were extended to non-state and individual actors, showing that the international system should not be analyzed solely from the viewpoint of interstate relations. Therefore, concepts previously considered immutable started being redefined (BUZAN; HANSEN, 2012).

Based on the premises of the constructivist strand, the Copenhagen School develops the theoretical concept of securitization. Perceiving the expansion of the field of international security, the School extends the concept of security beyond the political-military domain by introducing new sectors of analysis: economic, environmental and societal. To this end it analyzes discourses and security units to verify the securitization of a given topic.

Thanks to securitization theory, new forms of security analysis started being considered based on the discourse and stance of non-state and individual agents in the international system. That enhanced the perception and understanding of new international threats, previously linked mainly to the state (MOTTA, 2014). It allowed studies to be extended to the security of individuals and demonstrated cases of unbalance between state and society, such as when national minorities are threatened by the state itself or when the latter mobilizes society to face internal or external threats (BUZAN; HANSEN, 2012).

According to Grace Tanno (2003), security building processes start out from discourses by actors interested in establishing security agendas, and may thus undergo the securitization process. However, this process does not depend solely on securitization agents, for the proposal must be also socially acknowledged as a security threat. In other words, for a security situation to be created from discourse, the audience to which it is directed and who must provide the means required for the object to be securitized must voluntarily agree with the discourse, directing the act of securitization (AMARAL, 2008).

Therefore, securitization is understood as the process in which the state's existence is threatened, requiring emergency actions that may even exceed laws and political procedures (BUZAN; WEAVER; WILDE, 1998). Thus, cyber securitization can be interpreted as the process of emergency action against a potential threat in cyberspace. The actors in the cyber environment are states, institutions, industrial and business corporations, financial and services sectors, political and religious activist groups, digital criminals, among others. The variety and number of actors multiply as technology and access to information advance. Included among the actors are both those who will provide the securitization discourse and those who may be considered threats to state security.

The securitization process is better perceived in the military sector, since the latter is legitimized by the modern state's monopoly of power to protect the nation against threats to national security. Thus, the state is considered the object of reference while the military elites are the securitization actors in charge of determining actions against threats through speech acts (TANNO, 2003). The securitization process becomes evident at a time when cyberspace is recognized by defense documents as a strategic domain posing different threats.

The extent of threats and vulnerabilities will vary according to the relative and absolute capacities of those involved (BUZAN; WEAVER; WILDE, 1998). However, in the sphere of cyberspace, asymmetric capacities and the increasing vulnerability of critical infrastructures alter the nature of the threat, since the peculiarities inherent in cyberspace make it difficult to prevent cyberattacks.

Cyberspace expands the ways in which the state's organizational stability can be undermined; a case in point, the organization of the Arab Spring requires no further comment. Cyber actions with political motivations[6] which seek to destabilize the government in order to publicize a specific ideal can cause damage to other sectors of society, making securitization more complex and sensitive. Moreover, they can cause the loss of internal and external legitimacy of states that fail to securitize the political sector against cyber threats.

Economic threats can be considered as those "aimed at the economic sectors that guarantee the survival of the state and are essential to the war effort" (TANNO, 2003). Given the interdependence, threats to the economic stability of a state can be understood as global (BUZAN, WEAVER, WILDE, 1998). Thus, cyber threats that target economic gains by stealing bank information – whether at individual, corporate or state level, for example – can cause economic and financial damage to the state, as well as transfer such damage to other interconnected sectors.

Finally, even though it does not specifically address the information revolution in its security study, the Copenhagen School presents, through securitization theory, how, when and what consequences political actors perceive as an existential threat to security based on speech acts – or political discourses – creating an emergency security agenda. The cyber universe expands the range of threats, which actually become even less noticeable due to the aforementioned issues of anonymity and uncertainty. Such peculiarities of the new domain lead to new approaches in the securitization process.

4 Cyberspace in the defense white papers

In view of the possible gap between security, national defense steps; and the fast advance of technology, states have become concerned about protecting and reducing their vulnerabilities through steps capable of promoting some kind of state development in the sphere of security,

6 Political threats can be classified as intentional threats – when a state does not recognize the legitimacy of a foreign state/government or the government is rejected by a domestic group due to conflicts of distinct principles – and structural threats – when there are contradictions in the state's organizational principles (TANNO, 2003). According to Buzan, Weaver and Wilde (1998), political threats to a state are those that challenge national sovereignty, since a threat at political level can be transferred to other sectors (BUZAN; WEAVER; WILDE, 1998).

regarding specifically cybernetics. Given the new power arena represented by cyberspace, the securitization process in the defense white papers of Germany, France and Brazil is analyzed by acknowledging cyberspace as a strategic domain.

Germany

The document *White Paper on German Security Policy and the Future of the Bundeswehr*, published in 2016, describes the challenges to the country's security policy. With regard to threats, the issues addressed are terrorism, weapons of mass destruction, uncontrolled migration, inter-state conflicts, climate control, among others. Regarding specifically the cyber domain there is a clear concern with the state's vulnerabilities to potential cyberattacks. On this subject, the document claims that "urgent steps are needed to protect against threats" (GERMANY, 2016, page 36).

The German document does not provide a clear definition of cyber security. However, it presents the concept of information domain as the space in which information is generated, processed, disseminated, discussed and stored. According to the *White Paper on German Security Policy*, cyberspace is the virtual space of all IT systems linked or linkable at data level on a global scale.

The document points out the seriousness of cyberattacks to critical infrastructures that may have consequences for the civilian population, claiming that the effects of the attacks cannot be resolved in the foreseeable future, since there is trend for this issue to get worse. It also claims that cybernetics and the information domain are areas of strategic and international importance and response time must be improved to prevent cyberattacks and information operations, with cyber protection and defense as priority.

> We must take preventive steps to reduce this risk through confidence building and conflict resolution mechanisms.
> There are few areas where internal and external security are as closely intertwined as they are in cyber space. The threat situation in cyber space necessitates a holistic approach in the framework of cyber security policy. (GERMANY, 2016, p. 38).

With regards to the cyber sector, the *White Paper on German Security Policy* prioritizes the need to reduce the vulnerabilities of critical national infrastructures such as communication, energy and logistics systems. Regarding the threats addressed in the document, concern is raised about attacks by non-state actors, such as terrorist groups and organized crime, besides specialized individuals who could cause serious damage with minimal effort. Such threats confirm the concern with acts that may be brought about by non-state actors. Thus, individuals are perceived as international actors in the German document. That in itself would require a deep theoretical discussion on international relations, which goes far beyond the purposes and limits of this paper.

The document does not specifically address the relationship between cyberspace and the civil sphere, but stresses the importance of transparency between the public and private

sectors and the need for cooperation with other states. According to the *White Paper on German Security Policy*, only by means of cyber security policy and cyber foreign policy would an effective protection against cybercriminals and cyberattacks be achieved. The information obtained in the document is summarized in the following table.

Table 1 – Summary of information obtained from the *White Paper on German Security Policy*

Year of Publication	2016
Does the document include a clear definition of cyber security?	No
What does the document say about the cyber sector?	Area of strategic and international importance. Cyber protection and defense are prioritized.
What threats are considered?	Non-state actors. Terrorist groups, organized crime, individuals specialized in infrastructure damage.
What is the stance regarding the involvement of other civil sectors?	Not specified, but the need for transparency among sectors to fight cyber threats is stressed.

Source: Based on Germany (2016)

Germany considers the emergence of new threats as one of the factors behind the need to review its white paper, arguing that "new threats and hazards have emerged in addition to those that already existed" (GERMANY, 2016, p.15). Regarding threats stemming from the cyber domain, there is a section dedicated exclusively to fighting "Threats to Information and Communication Systems, Supply Lines, Transportation and Trade Routes as well as the Secure Supply of Raw Materials and Energy" (GERMANY, 2016, p. 41). In this section the prosperity of German society is seen as dependent on the use of global communications and information, and any "interruption of access to these global public goods on land, in the air, at sea, in the cyber and information domain, and in space involves considerable risks for the ability of our state to function and for the prosperity of our citizens" (GERMANY, 2016, 41).

The document defends the need to improve personnel and technology to enhance the state's performance in cyberspace. Perhaps as a consequence, in April 2017 the Cyber and Information Space Command (CIR) was created, which corresponds to the cyber branch of the German military (WERKHÄUSER, 2017).

France

The *French White Paper on Defence and National Security*, prepared in 2013 by the French government, expresses concern with cyberattacks – alongside threats of nuclear proliferation, pandemics and terrorism – already in first lines of the preface written by the then president François Hollande.

The document considers the growing insertion of French society in the media as a factor of vulnerability. In this sense, it emphasizes that universal access to cyberspace and the non-identification of perpetrators (the uncertainty issue previously discussed) are the main aggravating factors. In this context, allusions are made to threats in cyberspace, from cybercriminals to cyberattacks led by other nations. Such considerations reveal that in the French white paper cyberspace is understood as an essential environment for the state, a stage for potential challenges and conflicts. "The possibility of a major cyberattack on national information systems in a scenario of cyberwarfare constitutes an extremely serious threat for France and its European partners" (FRANCE, 2013, page 43).

Regarding the questions herein proposed for the comparative analysis, the *French White Paper on Defence and National Security* does not provide a clear definition of cyber security. However, it interprets cyberspace as a conflict area and considers it a strategic priority for protection against threats and attacks. Regarding threats, it considers both non-state actors and states capable of develop espionage and cyberattacks. Concerning the introduction of the civilian sector as an aid to national protection, the document, while involving other sectors of government – in addition to the Armed Forces – does not address the issue of civilian involvement. Table 2 presents a summary of the information obtained.

TABLE 2 - Summary of information obtained from the French White Paper on Defence and National Security

Year of Publication	2013
Does the document include a clear definition of cyber security?	No
What does the document say about the cyber sector?	Cyberspace is considered an area of confrontation and threats. It is perceived as having strategic priority for protection against cyberattacks.
What threats are considered?	Non-state, such as cybercrime and terrorism against state-owned companies. It considers the possibility of cyberattacks in a scenario of cyberwarfare.
What is the stance regarding the involvement of other civil sectors?	Despite involving other government sectors besides the Armed Forces, it does not address the issue of civil involvement.

Source: Based on France (2013)

In the case of France, no new threats are specifically considered. That is due, according to the French white paper, to the fact that the threats alluded to in the document were described in the previous 2008 version. However, the document addresses in its introduction the spread of risks and threats, including terrorism, cyber threats, organized crime, the proliferation of conventional and nuclear weapons. Pandemic, technological and natural risks are seen as strategic issues that may have serious repercussions for France (FRANCE, 2013, p.10).

The French white paper features a specific section on fighting cyber threats which, according to the text, are becoming more prominent with French society's increasing dependence on interconnected information systems. The ability to protect the country against cyberattacks is treated as a matter of national sovereignty. Thus, like the German document, the French white paper emphasizes the need to improve personnel and capability for cyberspace operations. As in the German case, there is no mention of the creation of COMCYBER, the cyberwarfare unit that became operational three years after the publication of the French white paper (REEVE, 2016).

Brazil

The transversality between new and traditional threats suggests the need to adapt the new themes to the Brazilian reality. Aiming to promote transparency and dialogue between national institutions, society and the international community in the sphere of defense, the *White Paper on Brazilian National Defense* ("Livro Branco de Defesa Nacional" – LBDN) proposes to be a mechanism for cooperation among South American countries.

In this sense, the cyber sector was included in the document as a national strategic priority, along with the nuclear and space sectors. The inclusion of the sector in LBDN is related to the creation of the document *Green Paper: Cyber Security in Brazil* ("Livro Verde: Segurança Cibernética no Brasil"), published in 2010. Previously developed to serve as reference for the creation of a *White Paper: Brazilian National Policy for Cyber Security* ("Livro Branco: Política Nacional de Segurança Cibernética"), the document features national strategic cyber security guidelines, besides suggesting efforts for international cooperation and dialogue, especially within the framework of the Organization for Economic Co-operation and Development (OECD).

The Green Paper defines and explains the main Brazilian strategic sectors in terms of opportunities and challenges that involve cyber security, namely: political-strategic, economic, social and environmental, ST&I, education, law, international cooperation and critical infrastructure security. Through them it proposes macro-coordination among sectors and inter-agencies operating in cyber security with the goal of strengthening the Brazilian cyber space. The abovementioned document also states clearly that the development of strategies and standards ensures increased incentives for research and innovation, generating human resources training, greater protection of critical infrastructures and national and international cooperation.

Aiming at structuring cyber security in Brazil, the Green Paper proposes an agenda of initiatives to

> [...] support and strengthen its activities in order to enable and expedite the formulation of policies, standards and regulations, research and development of methodologies and technologies, international cooperation and implementation and promotion of macro-coordination to integrate processes, aiming to ensure the availability, integrity, confidentiality and authenticity of information of interest to

> the Brazilian state and society, as well as the resilience of its critical infrastructures (BRASIL, 2010, p. 25, our translation).

Although the Green Paper did not meet the goal of launching the national cyber security policy, it enabled national cyber security strategic planning for the National Defense Strategy (END), for the National Defense Policy (PND) and, therefore, for LBDN. Its proposals promoted the protection and development of Brazilian cyberspace, especially by evidencing how important the subject is to other nations. Thus, the interest in attaching importance to the cyber sector resulted in the specification of premises for a cyber defense project and efforts for inter-agency initiatives, as provided in the 2012 LBDN. To this end, the White Paper assigns to the Brazilian Army the responsibility for cyberspace defense.[7]

Within the framework of Army coordination, the document provides for advances in human resources training, as well as the competence to act and protect cyberspace. In order to encourage advances and technological innovations for the defense industry, LBDN suggests the construction of national critical systems and components. In addition, the document indicates the Army Center for Cyber Defense (*Centro de Defesa Cibernética do Exército* – CDCiber) as the agent responsible for strengthening security, with authority to respond to cyber incidents, provide human resources training and protect Brazilian cyberspace. For such purposes, CDCiber operates together with other government agencies pertinent to the sector.

According to LBDN, the insertion of the cyber sector in the framework of strategic defense sectors aims to "ensure the confidentiality, availability, integrity and authenticity of data transmitted through their networks, which are processed and stored" (BRASIL, 2012, p. 71, our translation). Besides regarding it as a long-term goal, the document also indicates actions to be implemented in the short term due to the dynamic nature of the sector. These are: i) construction of the CDciber headquarters; ii) acquisition of infrastructure, support equipment and defense hardware and software solutions; iii) human resources training; iv) projects to structure the cyber sector.

It is therefore clear that LBDN comprehensively describes the features and competencies assigned to the cyber sector. Regarding concepts and definitions, it does not specify the themes that comprise the scope of cyberspace, hindering the consistency of information and formulation of terms for the performance of responsible bodies. Moreover, the threats to Brazilian cyberspace are not identified. Regarding the performance of other players in cyber defense, LBDN mentions only the participation of government bodies with previous connections with the sector.

7 According to the highest Brazilian defense documents (LBDN, PND and END) there are three strategic sectors for national defense: cyber – assigned to the Army; nuclear – assigned to the Navy; and space, assigned to the Air Force.

It is also noteworthy that the first edition of the *White Paper on Brazilian National Defense* was published in 2012; the second edition, of 2016, was only approved by Congress in December 2018.[8] This paper used as source the 2012 version and the 2016 draft, approved in its entirety by Congress.[9] Given the widespread use of information and communication technologies in Brazilian society, the 2016 LBDN draft draws attention to the challenges posed to the country by the hybrid or irregular nature of the "conflicts of the future," which combine regular combat action with information and cyber elements, carried out by both state and non-state actors. The emergence of cyberwarfare is also generally viewed as a challenge for Brazilian defense.

The LBDN draft argues that the "cyber threat has become a matter of concern for jeopardizing the integrity of sensitive infrastructures essential to the operation and control of various systems and agencies directly related to national security" (BRAZIL, 2016, p. 57, our translation). Even so it does not specifically define what a cyber threat might be. However, the cyber sector, together with the nuclear and space sectors, are still considered strategic and a priority for national defense.

The 2016 document still does not provide a clear definition of cyber security. Cyberspace is considered a priority as a medium through which damage can be caused to infrastructure and society, which is increasingly inserted in information and communication technologies. Regarding threats, the document briefly comments on the possibility of attacks by state and non-state actors, but does not delve deeper into identifying or characterizing them. Finally, with respect to involvement with the civilian sector, in addition to assigning to the Brazilian Army the responsibility for cyberspace defense, LBND involves other government and military sectors, considers participation in international forums and addresses the issue of civilian involvement through closer interaction of the Armed Forces with the private and academic sectors.

Therefore, one sees in these defense documents that the efforts to develop clear regulations and goals for operation in the cyber sector are in the initial phase. Little progress was made between the 2012 LBDN and the 2016 draft regarding goals, targets and aspiration. Given the dynamic nature of cyberspace and the speed with which threats change in the contemporary world, the mechanisms to fight cyberattacks must become effective and the documents must detail clearly the duties of the responsible body.

8 Legislative decree PDS 137/2018, which approved the new guidelines for the National Defense Policy (PND), the National Defense Strategy (END) and the review of the White Paper on Brazilian National Defense (LBDN), was published in the Federal Official Gazette on December 17, 2018.

9 For an in-depth analysis of the defense documents of Brazil and other South American countries, see *Guia de Defesa Cibernética na América do Sul* [Guide to Cyber Defense in South America], by Oliveira et al (2017).

TABLE 3 - Summary of information obtained from the *White Paper on Brazilian National Defense* (LBDN)[10]

Year of Publication	2016 (draft)
Does the document include a clear definition of cyber security?	No
What does the document say about the cyber sector?	The cyber sector is seen as a priority since cyberspace may be used to cause damage to infrastructure
What threats are considered?	State and non-state. There are no details about what those threats might be.
What is the stance regarding the involvement of other civil sectors?	It involves other government and military sectors and considers participation in international forums, but does not address civil involvement.

Source: Brasil (2016)

The most recent version of LBDN determines the creation of the Cyber Defense Command (ComDCiber) as a joint military organization, to which CDCiber and the National School of Cyber Defense (ENaDCiber) are subordinated. ComDCiber "has as its main responsibilities, among others, planning, guiding, supervising and controlling activities related to operations, intelligence, doctrine, science and technology, as well as providing training in the Cyber Defense Sector" (BRAZIL, 2016, p. 58, our translation). At this point an institutional advance of the cyber issue is identified in the Brazilian documents, due to the creation of a command that is more comprehensive and therefore more hierarchically qualified in terms of personnel, resources and infrastructure than CDCiber, as established by the 2012 LBDN version.

The creation of ComDCiber thus shows an evolution in the perception of the strategic value assigned to the cyber sector by the Brazilian government as a securitization agent. However, it is important to stress that this is not a branch of the Armed Forces as is the case with the German CIR and the French COMCYBER.

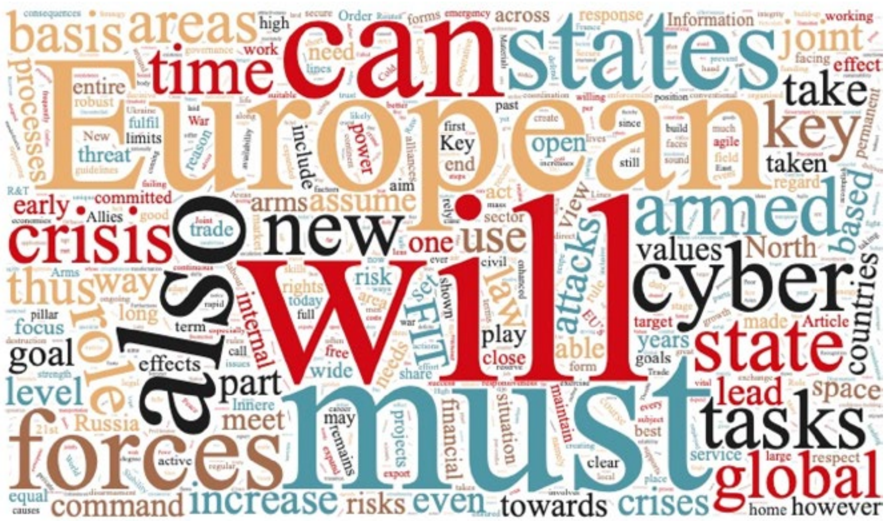
5 Comparative analysis of documents

The comparative analysis of the documents' contents aims to highlight the varying levels of importance attached to specific subjects by the states in question.

In order to highlight the importance of certain subjects in the documents, an automated word frequency count was performed in each white paper, resulting in the following word clouds:

10 Although this paper addresses both the 2012 and 2016 editions, for methodological reasons the summary analysis is restricted to the latter document, i.e., the most recent version of LBDN published by Brazil, as was the case with the analyses of Germany and France.

Figure 1 – Word cloud of the German Defense White Paper



Source: Based on Germany (2016)

The prominence of the European context over the national context is evident. It is also observed that the cyber theme appears with significant frequency in the text. This is due to the widespread use of the prefix "cyber" in the paper in words like "cyber threats," "cyberattacks," "cyberspace," among others.

Figure 2 shows graphically the most common words and subjects in the French document.

Figure 2 – Word cloud of the French Defense White Paper

Source: Based on France (2013)

A quick analysis shows the replacement of the term "European," highlighted in the analysis of the German document, by the word "world" in the French text. The term "cyber" does not have the same prominence in the French document as in the German document.

The word cloud based on the French white paper highlights a more imperative discourse compared to the German document, while the theme of threats appears more prominently throughout the text.

Figure 3 - Word cloud of the Brazilian Defense White Paper [11]

Source: Based on Brasil (2016)

The word cloud based on the 2016 draft shows the prominence of military participation in defense when compared to other countries. While the other white papers do not actually allocate tasks to different forces or civilian sectors, the LBDN draft is objective and categorical, preserving the areas of responsibility of each branch of the Armed Forces and determining the creation of ComDCiber.

Continuing the comparative analysis, table 4 features the total number of pages of the documents and the number of pages that address the issues of threats, new threats and specifically the cyber issue.

Table 4 – Comparison of white paper pages

	Total number of pages	Pages addressing threats	Pages addressing new threats	Pages addressing the cyber issue
Germany	143	24	1	28
France	135	52	0	23
Brazil	185	12	1	15

Source: Based on France (2013), Brasil (2016) and Germany (2016)

11 The incidence of prepositions is due to two factors: the peculiarities of the Portuguese language and the impossibility of excluding terms in the analysis tool employed..

As observed in the country-specific analysis, the categorization of "new threats" is almost non-existent, hence the disparity in the number of pages addressing "new threats" and "threats." This is due to the treatment given to non-state threats, which despite being new in the cyber domain, are categorized as threats by the defense documents. This fact indicates an advance in the securitization discourse of countries and contrasts with the conception of exclusively state-related threats.

Another relevant point is the greater number of pages addressing the cyber threat issue compared to threats, which is consistent with the current interpretation in the documents that cyberspace is not only a space of threats but also a strategic domain for the development of the analyzed countries.

The comparative approach also considered the key words present in the documents, which consisted of the following list: Defense, Security, Military, Army, Air Force, Navy, Terrorism, Drugs and Cyber (with their Portuguese equivalents for the analysis of the Brazilian document). The frequency with which these terms appear in the documents was then identified in order to highlight the prevalence of certain subjects over others.

Table 5 – Comparison of keywords

Key-words	Defence (Defesa)	Security (Segurança)	Military (Militar)	Army (Exército)	Air Force (Aeronáutica)	Navy (marinha)	Terrorism (Terrorismo)	Drogs (Drugas)	Cyber (Ciber)
Germany	53	99	49	2	0	0	13	0	28
France	136	136	83	2	2	4	18	2	24
Brazil	132	73	118	58	39	68	2	4	16

Source: Based on France (2013), Brasil (2016) and Germany (2016)

There is a greater prevalence of the cyber theme compared to the themes of terrorism and drugs, traditional subjects in defense documents. This is explained by the drug trafficking and terrorism activities developed in cyberspace, in parallel with the threats that arise in the cyber domain. Moreover, cyberspace is not categorized solely as a threat theme, as with the themes of terrorism and drugs, but as a strategic domain to be securitized and concurrently developed from an economic, social, governmental and civil point of view.

Also conspicuous is the involvement of the military sector in the Brazilian discourse, with the military and the different branches of the Armed Forces being mentioned much more frequently than in the other countries.

From the comparative analysis of the documents it is possible to identify political congruencies and divergences regarding the strategic valorization of cyberspace by nations that are developing their cyber defense policies.

In this sense, it is important to stress that among the analyzed countries Brazil is the only one without documents specifically focused on cyber security at the strategic level. Although the 2010 *Green Paper on Cyber Security* is a specific document that served as the basis for subsequent defense documents, no new documents have been created addressing the current reality of the

cyber sector. While Germany and France already have specific documents in force for the sector, *National Cyber Security Strategy* (GERMANY, 2016) and *National Cyber Security Strategy* (FRANCE, 2015), respectively, in the Brazilian case the document that addresses the cyber issue is the *Military Doctrine of Cyber Defense* (BRASIL, 2014).

6 **Conclusions**

Recurrent concern with threats posed by state and non-state agents, as well as acknowledgment of infrastructure and social vulnerabilities resulting from society's greater insertion in and consequent dependence on cyberspace, legitimize the latter as a stage for power relations nowadays. Therefore, the analysis of cyberspace securitization in the national defense white papers of Brazil, Germany and France contributes to determine and compare national defense and security strategies.

At a time when cyberspace is recognized as the stage for economic, political, military and social relationships, it is understood that the securitization discourse of states takes shape in their defense documents. In the documents consulted and analyzed, the cyber sector is considered a strategic and priority domain in which the threats and vulnerabilities to which a state is subject are defined (even if comprehensively). The bodies responsible for protecting the state in cyberspace are also defined. Other than that, the practice of identifying threats and objectives by securitization agents – in this case the state – agrees with the securitization process advocated by the Copenhagen School.

Therefore, the recurrent presence of the cyberspace issue and its recognition as a strategic and priority domain from the point of view of national defense legitimizes and justifies this study. Despite the theoretical challenges imposed by the particularities of cyberspace, it aimed to adopt a practical approach to the comparative analysis of the cyber sector in the defense white papers of Germany, France and Brazil. Therefore, it is understood that the perspectives of the Brazilian cyber sector should be further explored in order to guide the actions and responsibilities of the agents involved and offer possibilities of growth to cyber security in Brazil.

References

AMARAL, Arthur Bernardes do. **A Guerra ao Terror e a tríplice fronteira na agenda se segurança dos Estados Unidos**. 2008. Dissertação (Mestrado em Relações Internacionais) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2008.

AMORIM, Celso. Segurança Internacional: novos desafios para o Brasil. Contexto Internacional, Rio de Janeiro, v. 35, n. 1, p. 287-311, 2013.

BRASIL. Ministério da Defesa. **Livro Verde: Segurança Cibernética no Brasil**. Brasília, 2010.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília, 2012.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. Brasília, 2014.

BRASIL. Ministério da Defesa. **Minuta do Livro Branco de Defesa Nacional**. Brasília, 2016.

BRIDI, Sônia; GREENWALD, Glenn. Documentos revelam esquema de agência dos EUA para espionar Dilma. **Fantástico,** [S.l.], 1 set. 2013. Available at: http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html. Access on: 26/11/2018.

BUZAN, Barry; WEAVER, Ole; WILDE, Jaap De. **Security:** a new framework for analysis. Boulder: Lynne Rienner Publishers, 1998.

BUZAN, Barry; HANSEN, Lene. **A evolução dos estudos de segurança internacional.** UNESP: São Paulo, 2012.

CARREIRO, Marcelo. A Guerra cibernética: cyberwarfare e a securitização da Internet. **Revista Cantareira**, Niterói, RJ, n. 17, p. 123-137, jul./dez. 2012.

CEPIK, M.; CANABARRO, D. R.; BORNE, T. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: CEPIK, M. (Org.). Do 11 de setembro de 2001 à "Guerra Contra o Terror": reflexões sobre o terrorismo no século XXI. Brasília: Instituto de Pesquisa Econômica Aplicada, 2014. p. 161-186.

CHEN, T. **Cyberterrorism after Stuxnet**. Carlisle: United States Army War College Press, 2014.

COLLIN, B. Future of cyberterrorism: the physical and virtual worlds converge. **Crime and Justice International**, Chicago, v. 13, n. 2, p. 15-18, 1997.

DENNING, D. E. **Cyberterrorism**: testimony before the special oversight panel on terrorism. [S.l.]: Terrorism Research Center, 2000.

FARRET, Nerissa Krebs. A securitização do narcotráfico nos Estados Unidos e a influência no Brasil. **Conjuntura Global**, Curitiba, v. 3, n.2, p. 117-123, abr./jun. 2014.

FRANCE. **French White Paper on defence and national security**. Paris, 2013.

FRANCE. **National Cyber security Strategy. Paris**, 2015.

GERMANY. **White Paper on German Security Policy and the future of the Bundeswehr**. Berlin, 2016.

GERMANY. **National Cyber security Strategy.** Berlin, 2016.

GOLDANI, Carlos Alberto. **Malwares**. [S.l.]: Unicert Brasil Certificadora, abr. 2005.

HAESBAERT, Rogério. Território e multiterritorialidade: um debate. **Geographia**, Niterói, RJ, v. 9, n. 17, p. 19,46, 2007. Available at: http://periodicos.uff.br/geographia/article/view/13531/8731. Access on: 12 fev. 2018.

HILDEBRANDT, Mireille. Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace. **University of Toronto Law Journal**, [S.l.], v. 63, n. 2, p. 196-224, 2013.

KALLBERG, Jan; COOK, Thomas. **The unfitness of traditional military thinking in cyber**. **IEEE Access**, Piscataway, v. 5, 2017.

KENNEY, Michael. Cyber-terrorism in a post- Stuxnet world. **Orbis**, Amsterdam, v. 59, n. 1, p. 111-128, 2015.

KUEHL, Daniel T. **From cyberspace to cyberpower**: defining the problem. Washington, DC: National Defense University, 2009.

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

LOBATO, Luisa Cruz; KENKEL, Kai Michael. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, Brasília, v. 58, n. 2,p. 23-43, 2015.

MOTTA, B. V. C. **Securitização e política de exceção**: o excepcionalismo internacionalista norte-americano na segunda Guerra do Iraque. 2014. Dissertação (Mestrado em Relações Internacionais) – Universidade Estadual Paulista Júlio de Mesquita Filho; Universidade Estadual de Campinas; Pontifícia Universidade Católica de São Paulo, São Paulo, 2014.

NYE, Joseph S. **O futuro do poder**. São Paulo: Benvirá, 2012.

OLIVEIRA, Marcos Aurélio Guedes de. (In)Conclusão: Sobre a Necessidade de se Pensar a Defesa a Partir do Poder Cibernético. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo Bento; GONZALES, Selma Lúcia de Moura (Org.). **Segurança e Defesa Cibernética:** da fronteira física aos muros virtuais. Recife: UFPE, 2014. p. 193-196.

OLIVEIRA, Marcos Guedes de et al. **Guia de defesa cibernética na América do Sul**. Recife: UFPE, 2017.

POLLITT, M. Cyberterrorism: fact or fancy? Computer Fraud and Security, Amsterdam, v. 1998, n. 2, p. 8-10, 1998.

PRIVACY INTERNATIONAL. London, 1 Feb. 2011. Available at: https://bit.ly/2WdGYIU. Access on: 26 out. 2018.

REEVE, Tom. France unveils cyber command in response to 'new era in warfare'. **SC Media UK**, London, Dec. 2016. Available at: https://scmagazineuk.com/france-unveils-cyber-command-response-new-era-warfare/article/1475678. Access on: 21 dez. 2018.

SAINI, Hemraj; RAO, Yerra Shankar; PANDA, Tarini Charan. Cyber-crimes and theis impacts: A review. **International Journal of Engineering Research and Applications**, Ghaziabad, v. 2, n. 2, p. 202-209, mar-abr, 2012.

SYMANTEC. **Internet security threat report**. Mountain View, CA, abr. 2016. v. 21.

TANNO, Grace. A contribuição da escola de Copenhague aos estudos de segurança internacional. **Contextointernacional**, Rio de Janeiro, v. 25, n. 1, p. 47-80, jun. 2003. Available at: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292003000100002&lng=en&nrm=iso. Access on: 13 fev. 2019.

WEIMANN, Gabriel. Cyberterrorism: the sum of all fears? **Studies in Conflict and Terrorism**, Abingdon, v. 28, n. 2, p. 129-149, 2005.

WERKHÄUSER, Nina. German army launches new cyber command. DW, Bonn, 01 April 2017. Available at: https://p.dw.com/p/2aTfJ. Access on: 21 dez. 2018.

WIKILEAKS. **Espionnage Élysée**. [S.l.], 2015. Available at: https://wikileaks.org/nsa-france/. Access on: 27/10/2017

ZUCCARO, Paulo Martino. Tendência global em segurança e defesa cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. *In*: BARROS, O. S. R.; GOMES, U. M.; FREITAS, W. L. (org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 49-77.