ARTIGO

Discourses of cyberspace securitization in Brazil and in the United States

Discursos de securitização do ciberespaço no Brasil e nos Estados Unidos

http://dx.doi.org/10.1590/0034-7329201500202

*LUÍSA CRUZ LOBATO**
*KAI MICHAEL KENKEL***

Rev. Bras. Polít. Int. 58 (2): 23-43 [2015]

Introduction

The significant amount of virtual attacks against government websites, public and private confidential networks, and individuals highlights the risks of being online. These phenomena contribute to an environment which reaffirms perceptions such as that of a former US Deputy Secretary of Defense that "bits and bytes can be as threatening as bullets and bombs" (Lynn 2011). Denial-of-service (DDoS) attacks or worms like Stuxnet—designed to sabotage critical infrastructure and networks—stimulate discursive responses that contribute to what will be referred to as securitization of cyberspace.

The particular architecture of cyberspace facilitates anonymity, which hinders the tracking of many of the sources of such attacks, constituting an additional factor of insecurity which feeds catastrophic predictions related to internet vulnerability. At a time when trade and service infrastructure increasingly depend upon virtual systems, the illegal use of cyberspace is being perceived as a threat to national security. This has been the case of the United States (US) and the United Kingdom (UK), as well as of Estonia and Brazil.

Discourses which describe features of cyberspace as potential arenas for the emergence of threats to national security point to a broadening of the securitization process. While at the end of the Cold War network security was a matter for a select few electronics experts, in today's broadened debate, states, individuals and corporations are undeniable stakeholders. Cyberspace became crucial to security

* Pontifícia Universidade Católica do Rio de Janeiro, Instituto de Relações Internacionais, Rio de Janeiro – RJ, Brasil (l.cruzlobato@gmail.com).

** Pontifícia Universidade Católica do Rio de Janeiro, Instituto de Relações Internacionais, Rio de Janeiro – RJ, Brasil (kenkel.iri@gmail.com).

discourses, and in specific geopolitical contexts, came to be analyzed through a strategic and military perspective.

This article seeks to understand the manner by which these discourses of cyber securitization are constructed, using as examples the US and Brazil, and as its theoretical underpinning the approach developed by the Copenhagen School. Following the model developed by Hansen and Nissenbaum (2009), we suggest the development of a specific analytical "sector" for cyberspace, beyond the five originally developed by Buzan et al. (1998). The creation of such additional sector allows the securitization model to capture dynamics that are particular to online threats, separating them from other sectors' existing threats, and distinguishing clearly between securitization and militarization. The aim is to contribute to the debate concerning the cyber-sector (Hansen and Nissenbaum 2009; Hart 2011; Garcia and Palhares 2014).

The first section of this article highlights the specific nature of cyberspace and its place on the international security agenda. The second section problematizes Copenhagen securitization theory, arguing that its sectors do not capture the cybersphere's specific dynamics. Hansen and Nissenbaum's (2009) theoretical contribution is adopted to better grasp the role of cybersecurity in contemporary international security. The third section makes an empirical analysis of official documents and securitization practices in the US and in Brazil, which gives contours to the proposed sector's analytical potential. The final section considers the thin line between securitization and militarization. Since these phenomena deeply affect the everyday use of cyberspace, addressing these issues under the traditional rationale of international security is doomed to fail.

Cybersecurity and international relations

In March 2014, during the Crimea crisis, several NATO websites were hit with DDoS attacks, which suspended the Organization's cybersecurity website and breached a non-confidential e-mail network (Croft and Apps 2014). These attacks overwhelmed servers' capacities with illegitimate information requests originating from multiple sources—generally the so-called "zombie" computers remotely run by a central data processor. Similarly, cyberattacks were waged against Estonia in 2007 and Georgia in 2008, both during conflicts with Russia. In 2010, Iranian nuclear facilities were the targets of the Stuxnet worm, the first known online attack against industrial infrastructure (Deibert 2013). Virtual espionage scandals broke to unveil operations that surveilled the privacy of millions of individuals, as well as heads of state (BBC 2014), leading to a blackout of the Syrian internet in 2012 (Rohr 2014). US Senator Carl Levin drew attention to cyberattacks committed by government-supported hackers as 'aggressive actions in cyberspace' (Krasny 2014).

The cyberspace, the worldwide interconnected information networks and

communications infrastructure that spans the Internet, telecommunications networks, computer systems and the information they contain (Melzer 2011) is what connects these events. Though frequently treated as such, cyberspace and the internet are not synonyms: the former is an electronic/electromagnetic operational domain, the latter is the operational domain's central network based on computers (Levy 1999:17; Cepik et al. 2014:163).

These networks' inherent features hold a large potential to affect the political and strategic *status quo*, being characterized by the nonexistence of well defined borders between virtual and real, particularly in terms of causes and consequences. The physical architecture and the software protocols that shape cyberspace make anonymity easy. The increasing speed and reach of the media, connects states, corporations and individuals on a global scale; to which low-cost devices add a democratic facet (Deibert 2002; Betz and Stevens 2011). Combined, these characteristics create a permissive environment for anonymous agents—individually or in the name of governments—to breach confidential systems and networks. Such actions can be interpreted as challenges to state sovereignty, and to individual and private sector data security. Hence, "in global cyberspace, the interdependence and interconnectedness of massively networked users and devices irrevocably alters the traditional dynamics of cause and effect" (Betz and Stevens 2011:40).

The interconnectivity of computer systems and the absence of effective borders constitute lax structures used to foster political and military disruptions, since they hold the potential "to control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, and radars" (USA 2003:6-7). Considered to be exaggerated, some catastrophic projections in which networks are used by rival states, terrorists and criminals to cause suffering and to threaten critical-infrastructures are dubbed cyberdoom scenarios (Cavelty 2008:112).

Nonetheless, real-world cyberevents confirm what might otherwise remain in the landscape of hysteria, generating responses from governments and the international community. The Tallinn Manual on the International Law Applicable to Cyberwarfare (NATO 2013) broaches the extension of humanitarian law to virtual reality, underscoring growing concern over the economic, political and social reach, frequency and consequences of cyberattacks.

The anxiety over cyberattacks and the publication of the Tallinn Manual reveal that the international community has high stakes in information and communication technologies. Information security quickly gains importance in a context of increasingly lax access and publication. Assuring the inviolability of secret information rises as a priority on the cybersecurity agenda, "information's role in international relations and security has diversified and its importance for political matters has increased, mostly due to the proliferation of information and communication technology." (Cavelty 2012a).

Before the 1990s, cybersecurity remained restricted to computer experts. In light of developments in computing technology, virtual threats now reach society in general—a process that partially accounts for the globalization of cybersecurity (Hansen and Nissenbaum 2009). Bridging information security and the effects of potential attacks on industrial facilities, services and supply, cybersecurity joins the defense discourses and strategies of countries that are targets of massive cyberattacks or that to a varying extent depend upon computerized systems. According to Cavelty:

> [c]yber-security is both about the insecurity created by and through this new place/space and about the practices or processes to make it (more) secure. It refers to a set of activities and measures, both technical and non-technical, intended to protect the bioelectrical environment and the data it contains and transports from all possible threats. (Cavelty 2012b:5).

Resulting from multiple threats, cybersecurity has multiple referent objects (Deibert 2002). Highlighting four images that translate this dynamic, Deibert offers a novel understanding of online dynamics. First, cyberattacks can be directed against nations' collective identities, when these are revealed as primary referent objects (targets of threat). This applies, for example, to countries that feel their collective identity is threatened by the diffusion of internet access, such as China and Iran. Here, controlling internet access is seen as a counter-threat, like China's Great Firewall[1]. Threats from the internet or cyberspace favor non-traditional forms of violence, in particular those stemming from the fear of losing information or whose perpetrators are non-state actors. From this perspective, the state is the referent object. This same threat may also be directed against the privacy of individuals, and conducted both by states and corporations. Nonetheless, while these images do not drastically differ from the threats and referent objects established by securitization theory (Buzan et al. 1998), the fourth image better explains the new dimension of threats from cyberspace.

Here, Deibert (2002) argues that digital networks are themselves the referent object, converting to security-threats security system breaches; the loss, theft or the corruption of data; and the interruption of information streams. This dynamic allows for the construction of multiple referent objects, in the image of the networks. This view stresses socioeconomic, as well as policy-related structural vulnerabilities; public and private entities are equally vulnerable to cyberattacks, even though they themselves can also be the perpetrators. Deibert argues for the primacy of this fourth image over the long term. Network security is not only the referent object in a new cyber-sector, but it is also the foundation upon which the existence of other referent object is constructed.

1 The Great Firewall is a contested example; its ends are ambiguous and it is unclear whether the final aim is to protect Chinese culture or to control the local population's access to the internet.

In the field of information security, threats are dangers capable of exploring breaches in systems. A cyberattack is hence a human deed that explores the vulnerabilities of the virtual sphere, managing to harm informational systems or even, in light of modern life's online dependency, material daily life, (Cavelty 2012c).

Worms, in turn, illustrate two of the mechanisms that materialize cyber threats, and which can affect either virtual structures, the material world, or both. Worms are software that acts within hardware systems, exposing them to invasions and information theft. In the 1990s, the perception that key operational sectors mostly relied on software emanated precisely from these kinds of cyberattacks and system meltdowns (Cavelty 2012c). Some worms specifically serve aims of crime of espionage, resulting in theft of commercial and confidential information, while others intend to damage specific systems. In 1986, the Morris worm attack on ARPANET affected a large part of the internet, cementing the perception that systems are intrinsically vulnerable and leading to the creation of the CERT–Computer Emergency Response Team—under the aegis of DARPA—the US Defense Advanced Research Project Agency (Cavelty 2012c). Where Morris led to perceptions of insecurity over the Internet, 2010's Stuxnet fed the idea that cyber threats have material effects in the real world.

Developed to attack Siemens' control systems, Stuxnet damaged the centrifuges used in Iran's nuclear program. The work is the most successful cyberattack to date in terms of material effects. It had the greatest repercussion for speculations of cyberattacks' impact on critical services, supply systems, and the likelihood of cyberwars (Cavelty 2012c). Although not resulting on human damage, the Stuxnet episode illustrates the materialization of a virtual threat.

Several discourses and practices contribute to the constitution of cybersecurity threats as issues of global import (Deibert 2002; Cavelty 2012c). We seek to understand this process of constitution to analyze how security policies react to real or perceived threats, without losing sight of the fact that threat construction and response are co-constituted (Krause 1998:306). The following section describes the Copenhagen School's perspectives on securitization and sectorization, leading into Hansen and Nissenbaum's (2009) proposal to create a cyber-sector. Understanding the construction of cyber threats through the recognition of a cyber-sector attributes a particular dynamic to the process of securitization, also allowing a distinction between securitization and militarization trends that have perfused the broader construction of threats from cyberspace.

The Copenhagen School and the securitization of cyberspace

The Copenhagen School argues that a security threat is social construct—not subject to structuralist ontology (Wæver 2012). The militarist and statist bias of Strategic Studies is here opened up for new and diverse referent objects and critical, constructivist/post-structuralist outlook (Krause and Williams 1997). This research

emphasizes the ideas of speech-act securitization and sectors, shedding light on the process of construction and definition of threats (Krause 1998:306)—an increasingly relevant perspective in the case of cybersecurity.

Utilizing theory of securitization implies recognizing its theoretical limitations (Balzacq 2011:19; Cavelty 2008:24) and risks (Bigo 2007:21). It cannot postulate a specific notion of security; rather, in highlighting the role of discourse, a fine-grained application of such a theory seeks to grasp how a securitizing actor operates, as well as how a certain topic ascends to the security agenda. The approach embraces the societal variables of security, besides the process of constructing threats (Elbe 2007:36; Hansen and Nissenbaum 2009:1160). Notwithstanding, the unintended consequences of its inappropriate use contribute to increased *in*security, as well as to catastrophic policies regarding human security (Bigo 2007:3).

Securitization theory characterizes security itself as an objective and self-referential concept and practice (Buzan et. al. 1998:25), acquiring different meanings in different societies, according to actors' perceptions (Krause 1998:306). Threats are socially and discursively constructed, products of a semantic competition over the persuasion of an audience regarding the labeling of a given topic as a matter of security (Buzan et al. 1998:32). This broadens the notion of the referent objects beyond the state, and one of the theory's virtues is precisely its focus on society as a specific sector of security analysis (Buzan and Hansen 2009:36).

Securitization is intersubjective, discursive, intentional and performative, as well as non-discursive, non-intentional and removed from the locus of the action (Balzacq 2011). Certain problems become security issues when presented as threatening in an efficient manner (Balzaq 2011; Cavelty 2008). Buzan et al. (1998) underline that the analysis of security entails the distinction between referent objects, securitizing actors and functional actors. Referent objects like the state, the individual or a computer network are those who suffer the existential threat (Deibert 2002); securitizing actors are responsible to declare an existential threat to the object of reference. Several entities can fit this role, such as bureaucrats, political leaders, governments, groups of pressure, as long as they are imbued with authority to deliver the act of speech (Buzan et al. 1998; Cavelty 2008); finally, the functional actors affect the sectorial dynamic, while they influence decisions, but are not involved in the act of speech *per se*.

To securitize a given topic is to transfer it to the sphere of security, labeling it as an existential threat to a certain human collectivity (Buzan et al. 1998:24; Cavelty 2008:25). This move is based on hypotheses of the future: of what shall happen if a given policy is or is not adopted (Buzan et al. 1998). The process involves securitizing actors who speak in the name of referent objects and gain authority by directing their rhetoric to an audience that must accept the speech-act through which a topic is granted the "security" label (Balzacq 2011). There is competition around what should constitute both threat and security, the latter being considered

an essentially contested concept whose meaning is not objectively framed, but inherently disputed (Buzan et al. 1998). The content of security is constituted through a speech act, a discourse that securitizes and constructs referent objects as well as real or perceived threats which require that adoption of enhanced policy measures that escape the usual decision-making process, allowing the policy to go beyond established rules and regulations (Buzan et al. 1998:201). Speech-act theory is the basis for understanding the securitization process, since rhetoric lends strength, while constituting a threat in itself (Wæver 2012:53). Speech acts wed action and speech, in that saying becomes doing: speech acts can involve saying something, as well as acting while saying something, besides deriving an action from the act of speech itself (Austin 1962:12; Onuf 1989:83; Balzacq 2011:5). As such, the process of securitization requires the audience's acceptance of the threat (Buzan et al. 1998:25).

This analysis presents a discursive analysis of the securitization of cyberspace, based on specific texts such as, *inter alia*, official documents, speeches, and press articles. Governments whose infrastructure and daily lives are highly dependent upon digital networks, as well as think tanks, tend to figure as securitizing actors, for they perceive the destabilization of the networks in which their operations strongly confide as threats. Thus, the loss of information or of operational capacity ranks as an important threat to their stability. Likewise, in the economic sector, networks also tend to be securitized in their own terms or in reference to structures that depend upon them and to social groups (Buzan et al. 1998:100). In this case, the audience is both part of the process that constitutes the threat, as well as is varies according the logic applied for persuasion (Léonard and Kaunert 2011).

The Copenhagen School distinguishes five security sectors: military, political, economic, societal and environmental (Buzan et al. 1998). Each sector comprises particular referent objects, as well as securitizing and functional actors. Balzacq (2011) highlights the relational feature within the sectors, as well as their relevance to the constitution of the involved objects and actors. Practices thus involve intersubjective interpretations of a certain historical and cultural inheritance, and also of the structure that constrains them.

Discourses of cyber securitization cannot be removed from the practices that constitute cyberattacks, software and hardware breaches, and their use to conceal or reveal identities, just as "the discursive side of nuclear deterrence and arms control practices cannot be entirely understood without the missiles, bombs and organizational resources, which over time sustained its existence and importance" (Adler and Pouliot 2011:23). The discursive elements are influenced by daily-life activities that produce diversified perceptions in the actors. These perceptions are re-dimensioned to the virtual reality and projected in terms of *potential* disruptive events. Therefore, "it is relevant to conceive of discourse as practice and to understand practice as discourse" (Adler and Pouliot 2011:16).

Discourses on the security of cyberspace require the broadening of the traditional concept of security that focuses only on military power and states' ability to tackle threats (Walt 1991). The incorporation of information technologies into contemporary war fighting, hacker operations, threats to users' data and privacy, and the civil and the military interest in the area all justify the growing space cybersecurity has come to occupy in the field of international security. Since cyberspace goes beyond the logic of national borders (Cavelty 2012a), the constructed threat encompasses multiple referent objects (Deibert 2002), and requires the theorization of a peculiar sector in order to precisely contextualize processes that are typical to the phenomenon of securitization.

In the 1990s, securitization theorists did not perceive cybersecurity as an existential threat to states (Buzan et al. 1998). However, as consequence of the growing dependence of human societies upon networks, Hansen and Nissenbaum (2009) argue that cybernetic issues are already securitized, suggesting that the materialization of this process is highlighted through policy, institutional and strategic responses. The Estonian and the US examples are paradigmatic, given the launch of Estonia's Center for Cyber Defense and the establishment in the US, in 1996, of the Presidents' Commission for Critical Infrastructure Protection. It is paramount to mention that different cases call for different securitization processes, all assuming the central importance of audience acceptance. In dealing with cyberspace issues, this process is directed toward didtinct audiences: decision-makers, IT experts, the military and public opinion (Léonard and Kaunert 2011).

Beyond these multiple audiences, in the context of cybersecurity, it is possible to recognize how some states, acting as securitizing actors before domestic and international audiences, alert to the risks of cyberattacks and to the need to establish a specific agenda to deal with those matters, while other states' bureaucracies, for example in the military sector, participate in the construction of the threat. Most concerns over cyberwar stemmed from this universe (Cavelty 2012c). It is also plausible that private agents should seek to securitize cyberspace, although their presence usually takes the form of functional actors. In this sense, the press stands out for its coverage of cyberattacks, as does academia, which has made an extensive contribution to the debate over cyber threats, alongside technology companies and their clients.

This multiple constellation creates the necessity of a theoretical framework that comprehends the connection between discourses and the political and normative consequences of constructing virtual issues as security problems. The idea of a cyber-sector is relatively novel. It has been theorized as an attempt to revamp the Copenhagen approach given the importance cybersecurity has acquired, reinforcing the idea that it has been successfully securitized (Hansen and Nissenbaum 2009; Hart 2011; Garcia and Palhares, 2014). Politically, this translates into institutional and discursive developments that, for instance, under the Clinton administration

in the US have engendered the creation of the aforementioned Commission on Critical Infrastructure Protection, as well as the formulation of national strategies oriented towards cyberspace (USA 1999; 2003; 2011; Brazil 2012).

Different discourses entail different threats, referent objects and securitizing actors. For Hansen and Nissenbaum (2009), there are three patterns of security within the cyber-sector: first, hypersecuritization, which represents the extension of securitization beyond regular levels of risk and threat, typically characterized by chain effects that have the capacity to reach other sectors. This pattern comprises catastrophic scenarios that usually contain projections of cascading disasters. The leverage of this discourse results from the hypothesis that damage to networks would yield radical effects in the societal, military and financial arenas, through scenarios that resemble environmental catastrophes.

Secondly, daily practices of security refer to the impact of virtual threats in the everyday life. The hypersecuritization landscapes gain even more plausibility, for catastrophe is usually associated with the disturbance of daily habits, such as the risks of virus-infected computers. This demands responsible behavior from Internet users, turning this group of interconnected people into audiences for both the potential enhancement and reduction of insecurity in the system, since these third parties can be instrumentalized for DDoS attacks (Hansen and Nissenbaum 2009:1166).

Finally, the pattern of technification creates discursive space for experts given the need for people with specific knowledge about systems operation. Technification legitimizes cyber securitization, supporting hypersecuritization discourses and aiming to influence public opinion in favor of those who master certain machines and the architecture of certain systems: "the mobilization of technification within a logic of securitization is thus one that allows for a particular constitution of epistemic authority and political legitimacy" (Hansen and Nissenbaum 2009:1167). The constitution of the expert's authority also leads to a separation between the "good science" of data processors and the "bad knowledge" of hackers. Cyber securitization involves a two-fold movement: from the political to the securitized; and from the political to the technical (Hansen and Nissenbaum 2009).

While Hansen and Nissenbaum (2009) consider interconnectivity an idiosyncrasy that unites an entire constellation of referent objects, one can infer that the networks that underpin systems and services constitute a referent object common to scenarios of hypersecuritization, of everyday practices and of technification. This is not to say that there are no referent objects interrelated through the network, but rather that securitization frequently happens to foster its integrity. Even different possible referent objects, are generally thought of in relation to the network itself: interconnected states and collectivities, networks of business and computers, governmental (confidential information), military and critical infrastructure networks (dependent upon hardware systems). Moreover, although

the authors emphasize the link between cyber and military securities (Hansen and Nissenbaum 2009:1162-1164), they do not elaborate on their differences. This distinction is of the utmost importance since it allows differentiation between security logic and military logic—which will be discussed below.

According to Buzan et al. (1998:70), the military sector is pervaded by the logic of friend versus foe, and by the centrality of states and political organizations similar in their insistence upon territorial integrity. While phenomena such as Stuxnet in Iran may bring the logics of the cyber-sector and military sector closer together, accentuating the perceptions of friend versus foe, and of the protection of a territorial integrity, they nevertheless differ perceptibly, since the former sees networks as major referent objects or as links to identify other objects.. There are no clear-cut divisions, due precisely to the organization of the networks themselves (Hansen and Nissenbaum 2009:1161). Cyberspace is an open space in terms of concurring risks and solutions. The Hansen and Nissenbaum discursive construction of threats and of referent objects does not necessarily imply the adoption of a military logic of security.

In securitization, a successful speech-act stems from the combination of language and inter-subjectivity (Buzan et al. 1998:32) with conditions that facilitate their interaction. These can be internal (the speech-act must follow a security grammar) or external (the social conditions of the securitizing actor and the likelihood of the acceptance of their speech, as well as the features of the threats that hinder or facilitate securitization). This is essential for the analysis of the content of specific securitizing actions, such as official documents, as well as for grasping how the utilization of the cyber-sector and the three patterns above contribute to understanding the construction of threats and vulnerability in cyberspace.

The analysis of American and Brazilian securitization discourses

This section addresses American and Brazilian discourses of securitization, based on national policy documents and on media accounts, with the intent of identifying to which audience these speech-acts were aimed, their referent objects, the presumed existential threat and the proposed responses. The discursive analysis identifies patterns of hypersecuritization, of securitization of everyday practices, and of technification, and the level of securitization of each of the cases is compared.

The United States

In the case of the US, the discourse of securitization is no novelty, having already gone through several phases. In the early 1990s, the country migrated from a process of cybersecurity politicization, or its introduction into the political agenda and debates, to securitization itself (Cavelty 2012a). Nonetheless, both

the Clinton (USA 1999) and George W. Bush (2003) Administrations, in their official discourses, witnessed – or practiced – pervasive securitization moves. The criteria for the prevention and reduction of risks from cyberattacks were institutionalized via the International Strategy for Cyberspace (2011) during the Obama Administration. The most recent strategy adopts a view in which cyberspace is the source of both opportunities and threats, derived from the interdependency and interconnectivity of networks. Thus, damage to cables, servers and networks caused by natural disasters, accidents or even sabotage, the spillover of material conflicts to cyberspace, as well as several types of cybercrimes are examples of threats that transcend national borders from virtual platforms:

> (…) low costs of entry to cyberspace and the ability to establish an anonymous virtual presence can also lead to "safe havens" for criminals, with or without a state's knowledge. Cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace (USA 2011:5).

The document shows an effort to publicize the securitization of cyberspace, an intention derived from the focus on government officials and industry. Cybersecurity as a matter of national security seems to have been internalized in the media, while cyberattacks, including DDoS, and the development of sophisticated viruses are frequently portrayed as 'weapons' and 'acts of war' threatening the security of US and allies' networks (Deibert 2013).

Patterns of hypersecuritization, of everyday practices and technification thrive in light of the proliferation of cybercrimes; viruses and worms that are capable of suspending the operation of industrial and commercial facilities; of attacks that affect the privacy of industry and individuals; and, at the national or international level, raise the risk of virtualization of material conflicts.

The document explicits to the public the implications of this threat to national security and to the private sector, as well as to everyday life. Network stability is central to the strategy, "… a cornerstone of our global prosperity, and securing those networks is more than strictly a technical matter" (USA 2011:9). Their instability and vulnerability threaten individuals, the private sector, governments and international society (USA 2011; Hansen and Nissenbaum 2009; Deibert 2002); threats may originate from terrorists, cybercriminals or even other states (USA 2011:12). However, while the sources of threats are attacks on networks and systems, many of these actors may operate as functional actors. The logic would be similar to what Buzan et al. (1998) sketch out using a company that pollutes the environment: these actors directly influence the dynamic of the cyber-sector, but they are neither referent objects nor securitizing actors, though they may contribute to actions that impact the perception of the threat.

The threat to networks that support critical infrastructures is portrayed in relation to the country's sovereignty and to the security of the population. This discourse is also legitimized for the particular features of the cyberspace, or appealing to traditional threats, such as terrorism and aggression. The reference is indeed relevant, since both securitization and the cyber threats interact in threat scenarios (Buzan et al. 1998), adopting the assumption of an acquiescent audience not entirely aware of the dangers (Hansen and Nissenbaum 2009). The document resorts to deterrence, as well as to the use of force, as possible responses to cyber threats (EUA 2011:14). It is important to highlight that the military sector has a significant role in the way cyber threats are perceived and managed—a trend that has increased in the debate on cybersecurity since the 1990s (Cavelty 2012c).

Beyond the above document, President Barack Obama's official discourses stressed the importance of placing cybersecurity among matters of national security, defining cyberspace as a strategic asset (EUA 2009), hence demonstrating its institutionalization in policy programs and an attempt to gain audiences in other security sectors. In 2010, the "*Protecting Cyberspace as a National Asset Act*" (PCNAA) was brought before the US Senate, seeking the assignment to the Federal Government of extensive responsibility in emergencies involving cybersecurity, including the power to intervene in the private sector (PCNAA 2010). Although the bill has not yet been voted upon, in the intelligence field, similar interventions led by the National Security Agency have already taken place without formal provisions.

Brazil

The number of cyberattacks against Brazil has been rising. In 2001, governmental websites were the targets of diverse attacks that disrupted website configuration or stole information (G1 2011). Estimates suggest that that country loses roughly USD 8 billion a year to cybercrimes (SYMANTEC 2012), while it is also a target of US espionage (Greenwald et al. 2013). Cyberattacks, cybercrimes and cyber espionage are interpreted as threats to digital networks, to individuals and to national security. In 2008, cyberspace was framed as a strategic sector within Brazil's National Defense Strategy (Brazil 2008). In 2012, the Ministry of Defense (MoD) released a Cyber Defense Policy (PCD), emphasizing the strategic level of cyber defense and the operational and tactical levels of cyberwar, aimed at guaranteeing human capital and expertise, reinforcing the security of public networks, developing intelligence capabilities, and the country's 'dissuasive capacity' (Brazil 2012:13).

The document establishes guidelines for the policy implementation including the creation of the Military System for Cyber Defense, the introduction of cyber defense in the joint exercises and combat simulations (Brazil 2012:16), as well as the issuing of federal legislation on the issue. Speaking of civilian and military

arenas, the document focuses on the fact that the efficiency of cyber defense depends on the level of awareness of the value of information that organizations and people possess or process (Brazil 2012:11). Informational assets are the referent objects, and emphasizes the need to reinforce network security through the spread of technical knowledge to strengthen defense capacity, as well as the country's counterattack capacity. On a daily basis, there is concern over the defense of banks' and corporations' networks, as well as over avoiding the utilization of personal computers for DDoS attacks and spam activities.

The existential threat to networks is legitimized in reference to national defense interests, considering the relationship between the stability of infrastructure and the information that sustains them, as well as to national vulnerability. As a political response, the document proposes a collaborative action including the MoD, the academia, public and private sectors and pillars of industrial defense. (Brazil 2012:11). For Lopes (2013), the securitizing movement has gained momentum in policy-making debates and in official documents. However, the application of the PCD's guidelines has been rather limited, in the continued absence of specific legislation for cyber defense (Brazil 2010:39). In its turn, the level of expertise within the intelligence community, another basis for mechanisms of cyber defense (Brazil 2012:16), is still far from attaining the necessary level to confront current threats (Gonçalves 2012:310).

Progress was made with the implementation of the National Cyber Operations Simulator (Simoc) at a cost of R$5 million (Portal 2013), aimed at training the military in cyber combat. Similar simulations are offered in academe, seeking to trigger the interest of data processing professionals in cybersecurity (DFTV, 2014). Furthermore, in 2014, R$ 40 million were set aside for the creation of a Cyber Defense School (Portal 2014). In 2010, Brazil created a Center for Cyber Defense (CDCiber) within the Army (Cepik et al. 2014:171), which has been centralizing Brazil's national cyber defense activities.

The following table illustrates the succession of documents and governmental agencies assigned to deal with cybersecurity in both studied countries, with an eye to tracking their institutional developments and securitization processes.

Table 1 – Main documents and governmental agencies assigned to deal with cybersecurity

	Documents	Agencies
USA	1999: A National Security Strategy for a New Century. 2003: The National Strategy to Secure Cyberspace. 2009: Remarks by the President on Securing our Nation's Cyber Infrastructure. 2011: International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.	Department of Homeland Security • Office of Cybersecurity & Communications • National Cybersecurity Division • Department of Defense • U.S. Cyber Command (USCyberComm) • National Security Agency (NSA)
BRAZIL	2008: National Defense Strategy (Law nº 6.703, 12/18/2008) 2012: Cyber Defense Policy (ordinance nº 3.389/MD, 12/21/2012)	ABIN – Brazilian Agency for Intelligence MD – Ministry of Defense • EB – Brazilian Army • CD Ciber (Center of the Army for Cyber defense) • Presidency of the Republic • Chamber of External Relations and National Defense (CREDEN) • Council for National Defense (CDN) • Department of Informational and Communication Security (DSIC) • The Presidency's Cabinet for Institutional Security (GSI-PR)

The chosen cases present differences and similarities with regard to the adoption of the securitization discourse, securitizing actors, and audience reception. While both present patterns of hypersecuritization, everyday practices and technification in threat construction, the primary referent objects are the digital networks that host critical infrastructure and services and connect people. These networks are securitized in terms of individual users and the governments and services that depend upon them. However, there are clear differences in how well-developed these processes are from country to country. In Brazil, cybersecurity is institutionalized (Cepik et al. 2014:171), grasped as a broader activity than defense, and is under the purview of the Presidency (Brazil 2010:50), making it safe to assume that there is a securitizing process (Lopes 2013) that still lacks major audience recognition. In the US, the process is consolidated, and permeates governmental practices, serving as a justification for the enhancement of vigilance mechanisms, as well as of state control.

The enlargement of the security framework to include threats beyond war highlights the applicability of Agamben's (2004) state of exception to responses such as of the US, characterized by growing regulations and surveillance in cyberspace. The state of exception enters everyday life via the generalization of security discourse as the government's *modus operandi*. The risks are higher when the discourse of securitization makes strong recall to the military sector: "the latest trend is to frame cybersecurity as a strategic-military issue and to focus on countermeasures such as cyber offence and defence, or cyber deterrence" (Cavelty 2012b:104).

Conclusions

The first section placed cybersecurity in the international relations context, exploring cyberspace as a space of flows where anonymity is a reality and borders a fiction. It presented how this area challenges visions of the international still based on the domestic/international divide. Significant global phenomena yield the perception of cyberattacks as threats to the privacy of individuals, economies and national security, triggering processes of securitization by countries that depend on these networks. The second section applied to this dilemma the theory of securitization, underlining the need to approach the topic via a distinct cyber-sector. The third section shed light on American and Brazilian securitization discourses, stressing that each case had different levels of securitization: in Brazil, it is a slow and restricted process, while it has been relatively swifter in the US, where there is an additional concern – the militarization of cybersecurity.

The discourse of danger converts cyberspace into a threat and has been shaped in the military arena (Cavelty 2012c), being increasingly present in the everyday life of people and businesses. The globalization of information and technological innovations enhanced the connectivity and complexity of systems, heightening uncertainty and vulnerabilities. In discourse, dependence upon informational infrastructure renders society vulnerable to attacks targeting networks and informational systems, jeopardizing the stability of the networks and systems that enable modern activities, from medical services and industrial facilities to general supply chains. In these cases, they can affect the material world, as did the Stuxnet worm (Cavelty 2012c).

The securitization of cyberspace is not controversy free; it remains less urgent in countries less dependent on information systems, and happens in the context of threats whose catastrophic proportions are still matters of speculation and guesswork. Cyberattacks and cyber espionage are very much real, but there is an escalation in the perception of threats involving the actions of hackers and cybercrimes, as well as online sabotage and cyberwar. This trend allocates energies and resources to preventing rather unlikely events from becoming reality (Cavelty 2012b), counting on the support of US political circles prone to extending the

security of the state at the expense of the security of individuals and their networks (Deibert 2002).

In the 1990s, countering cyber threats took on a political dimension, entering a context of competition for resources and influence that drove a tendency to overstate threats. Policymakers' and specialists' perception of risks is influenced by the potentially catastrophic effects of cyberattacks and by scenarios projected in literature, films and by think tanks (Libicki 2011). The so-called "bad use" of cyberspace threatens the social fabric in light of the perception of dependence and vulnerability of informational and telecommunications systems. In this sense, the media tends to distort the perception of threats when portraying virtual risks as increasing, constructing a threat of great proportions that is securitized and, in the US case, has led to militarized solutions and discourse.

The movement that shifts securitization to militarization raises concerns not only because the US are the global superpower, but also because the discourse of cyber securitization originates in the country, which has shaped a perception of the threat and possible countermeasures that are emulated in other countries. Even in Brazil, where there is only an incipient securitization process under way, the quest for military strategy, deterrence and operational guidelines stresses the trend to draw parallels between conventional military operations and the virtual world. Cavelty (2012b) argues that the deployment of military terminology such as cyberwar represents the existence of a rationale under which virtual challenges and threats are deemed resolvable as if cyberspace were an operational system.

The militarization of cyberspace is based on the fear that the capacity of states and non-state actors might seriously affect the usability of the internet. Although many fears over a virtual Pearl Harbor remain rhetoric, the likelihood of this perception triggering an "arms race" in cyberspace engenders the proliferation of cyber espionage, the dissemination of malwares, online surveillance, and several other forms of cyberattacks by states themselves: "in the rush to reject alarmism about cyberwar, we should not lose sight of the very real geopolitical conflict that has insinuated itself into this domain and threatens to subvert its architecture" (Deibert 2010).

It is not wise to intertwine securitization and militarization, especially since several countries present processes of securitization, while not necessarily linking it to militarization. However, it is still relevant to question the necessity and the limits of the process of securitization itself. Many discourses still employ traditional logics of security that are not quite adequate for virtual reality, as presented in this article. Cyberspace does not graft well onto security, and, therefore, analogies are dangerous. The state is not necessarily an actor whose innate capabilities provide it with the capacity to provide satisfying responses to challenges from cyberspace. The state's role in this domain is rather limited, even if a certain aspect of virtual reality is considered a first-line threat to national security (USA 2011), because

cybersecurity is a sphere that is shared by the private and the public sectors, and is exploited also by individuals. State actions to control cyberspace risk several freedoms and rights of all other actors.

Creating a distinct cyber-sector would allow subsequent analysis both to pinpoint the multiple constellation of actors, discourses and practices, and to reinforce the identification of patterns of hypersecuritization triggered by states that are dependent upon information networks, permitting the recognition of a separate security dynamic in actors' practices and discourses. One of the limitations of securitization theory is the conception of measures of urgency via policies of exception. It is questionable to conceive security policies as pathways to extraordinary circumstances that differ from everyday life: "Exceptional measures are highly contextual and subjective, so that they might not always be security measures in a restricted sense, and security measures might not always be exceptional" (Cavelty 2008:137). Exceptionality may turn into an excuse to practice governmental cyber espionage, and such a practice can become be normalized without leaving the logic of security (Agamben 2004).

Cyberspace portrayed threats that justify the logic of cybersecurity are just as concrete as others embraced by the other Copenhagen sectors. However, their essence cannot be fully grasped, let alone reasonably managed, without threating the access to virtual resources. This does not mean that dealing with this particular and complex space is impossible, but only that the responses to these challenges must respect the distinctness of cyberspace. As a form of power which deeply shapes the relationship between society and state, security analysis would benefit from openness to new ways of making sense of a world where the real and the virtual are increasingly interconnected. The potential cost of blindness to the specificities of cyberspace is high: decreased real security in the interstices of the concepts used to define and provide it.

Bibliographic references

Agamben, Giorgio. (2004) *Estado de Exceção*. São Paulo: Boitempo, 142p.

Adler, Emanuel and Pouliot, Vincent. (2011) *International Practices. International Theory*, vol.3, n.1, 2011, p.1-36.

Austin, John L. (1962), *How to Do Things with Words*, M. Sbisà and J. O. Urmson (eds.), Oxford: Oxford University Press, 166p.

Balzacq, Thierry. (2011) A theory of securitization: origins, core assumptions, and variants. In *Securitization Theory: How Security Problems Emerge and Dissolve*. Balzacq, Thierry. ed. Nova York: Routledge, p.1-30.

BBC (2014). Edward Snowden: Leaks that exposed US spy programme. *BBC News*. [http://www.bbc.com/news/world-us-canada-23123964] Accessed: 01/10/2015.

Betz, David J. and Stevens, Tim. (2011) *Cyberspace and the State: Toward a Strategy for Cyber-power*. New York: Routledge, 158p.

Bigo, Didier. (2007) Detention of foreigners, states of exception, and the social practices of control of the banopticon. In *Borderscapes: hidden geographies and politics at territory's edge*. Rajaram, Kumar; Grundy-Warr, Carl. eds. Minneapolis: University of Minnesota Press, p.3-34.

Brazil. (2012) *Ministério da Defesa*, Política Cibernética de Defesa aprovada pela Portaria Normativa No.3.389 de 21 de dezembro de 2012 (Brasil). [http://www.defesa.gov. br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf] Accessed 01/12/2015.

Brazil. (2008) *Presidência da República*, Decreto nº6.703 de 18 de dezembro de 2008 que aprova a Estratégia nacional de defesa. (Brasil). [http://www.planalto.gov. br/ccivil_03/_ato2007-2010/2008/Decreto/D6703.htm] Accessed 01/12/2015.

Buzan, Barry; Hansen, Lene. (2009). *The Evolution of International Security Studies*. Cambridge: Cambridge University Press, 368p.

Buzan, Barry; Wæver, Ole; De Wilde, Jaap. (1998) *Security: A New Framework for Analysis*. Boulder: Lynne Rienner, 239p.

Cavelty, Myriam Dunn. (2008) *Cyber-security and threat politics: US efforts to secure the information age*. Nova York: Routledge, 182p.

Cavelty, Myriam Dunn. (2012a). The Militarisation of Cyberspace: Why Less May Be Better. In. *2012 4th International Conference on Cyber Conflicts*. C. Czosseck, R. Ottis, K. Ziolkowski. Eds Tallin: NATO CCD COE, 2012, p.141–53.

Cavelty, Myriam Dunn. (2012b). The Militarisation of Cyber Security as a Source of Global Tension." In *Strategic Trends Analysis*, p.103–24. [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2007043]. Accessed 01/19/2015.

Cavelty, Myriam Dunn. (2012c) Cyber-Security. *Contemporary Security Studies, Allan Collins, Ed., Oxford University Press, 2012, p.1-33*. [http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2055122]. Accessed 01/15/2015.

Cepik, Marco; Canabarro, Diego Rafael; Borne, Thiago. (2014). A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In *Do 11 de setembro de 2001 à guerra ao terror: reflexões sobre o terrorismo no século XXI*, SOUZA, André de M.; Nasser, Reginaldo M.; Moraes, Rodrigo F. eds. Brasília: IPEA, p.161-186.

Croft, Adrian; Apps, Peter. (2014) NATO websites hit in cyber attack linked to Crimea tension. *Reuters* [http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316]. Accessed 01/09/2015.

Deibert, Ronald J. (2002) Circuits of Power: Security in the Internet Environment. In *Information Technologies and Global Politics the Changing Scope of Power and Governance,* Rosenau, James N., and J.P Singh, eds. Albany, NY: State University of New York Press, 2002. 115-142.

Deibert, Ronald J. (2010) Militarizing Cyberspace: To preserve the open Internet we must stop the cyber arms race. *MIT Technology Review* [http://www.technologyreview.com/notebook/419458/militarizing-cyberspace/]. Accessed 01/19/2015.

Deibert, Ronald J. (2013) *Black code: inside the battle for cyberspace*. Toronto: McClelland & Stewart, 525p.

DFTV 1ª Edição.(2014) *Guerra cibernética estimula estudantes ao mercado de segurança digita*l [http://globotv. globo.com/rede-globo/dftv-1a-edicao/v/guerra-cibernetica-estimula-estudantes-ao-mercado-de-seguranca-digital/3700806/]. Published: 10/16/2014. Accessed: 01/10/2015.

Elbe, Stefan. (2007) *HIV/AIDS and security. In Contemporary security studies*, Collins, Allan org. Oxford: Oxford University Press, p.331-345.

G1. (2011) *Veja lista de sites do governo afetados por onda de ataques virtuais* [http://g1.globo.com/tecnologia/noticia/2011/06/veja-lista-de-sites-do-governo-afetados-por-onda-de-ataques-virtuais.html] Accessed 02/09/2015.

Garcia, S.M.A; Palhares, A.I.D. (2014) Reflections on the virtual to real: modern technique, international security studies. Cyberspace *and International Relations: Theory, Prospects and Challenges*. Kremer, Jan-Frederik and Benedikt Müller, eds. Berlin: Springer, 284p.

Gonçalves, Joanisval Brito. Brasil, serviços secretos e as relações internacionais: conhecendo um pouco mais sobre o grande jogo. In *Defesa Nacional para o Século XXI: Política Internacional, Estratégia e Tecnologia Militar.* Silva Filho, Benedito da; Moraes, Rodrigo F. orgs. Rio de Janeiro: IPEA, 2012.

Greenwald, Gleen; KAZ, Roberto; Casado, José. (2013) Espionagem dos EUA se espalhou pela América Latina, *Jornal O Globo* [http://oglobo.globo.com/mundo/espionagem-dos-eua-se-espalhou-pela-america-latina-8966619] Published: 07/09/2013. Accessed 02/09/2015.

Hansen, Lene; Nissenbaum, Helen. (2009) Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly*, vol. 53, p. 1155–75 [http://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf] Accessed: 01/10/2015.

Hart, Catherine. (2011) Mobilizing the Cyberspace Race: the Securitization of the Internet and its Implications for Civil Liberties. *Cyber-Surveillance in Everyday Life*: An International Workshop, may 12-15, 13p. [http://www.digitallymediatedsurveillance.ca/wp-content/uploads/2011/04/Hart-Mobilizing-the-Cyberspace-race.pdf] Accessed 02/09/2015.

Krasny, Ross. (2014). Chinese hacked U.S. military contractors, Senate panel finds. *Reuters* [http://www.reuters.com/article/2014/09/18/usa-military-cyberspying-idUSL1N0RI1N420140918]. Published: 09/14/2014. Accessed 05/10/2015.

Krause, Keith. (1998) Critical Theory and Security Studies: The Research Programme of 'Critical Security Studies.' *Cooperation and Conflict*, vol. 33, p. 298–333.

Krause, Keith; Williams, Michael C. (1997) From Strategy to Security: Foundations of Critical Security Studies. In *Critical Security Studies: Concepts and Cases*. Krause, K.; Williams, M. eds. Minneapolis: University of Minnesota Press, p.33-60.

Léonard, Sara; Kaunert, Christian. (2011) Reconceptualizing the Audience in Securitization Theory. In *Securitization Theory: How Security Problems Emerge and Dissolve*. Balzacq, Thierry. ed. Nova York: Routledge, p. 57–76.

Levy, Pierre (1999). *Cibercultura*. São Paulo: Editora 34, 250p

Libicki, Martin C. (2011) Chinese Use of Cyberwar as an Anti-Access Strategy. Two Scenarios. In *RAND Testimony Series*, p.1-4. [http://www.rand.org/content/dam/rand/pubs/testimonies/2011/RAND_CT355.pdf]. Accessed 01/13/2015.

Lopes, Gills. (2013). Securitizando o ciberespaço: um estudo comparativo sobre a defesa cibernética em sete países. In *Anais do 4º Encontro Nacional da ABRI* [http://www.encontronacional2013.abri.org.br/conteudo/view?ID_CONTEUDO=877]. Accessed 01/12/2015.

Lynn, William J. (2011) The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack. *Foreign Affairs* [http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later]. Accessed 01/10/2015.

Melzer, Nils. (2011) *Cyberwarfare and International Law: Ideas for Peace and Security*. Geneva: UNIDIR, 38p.

NATO. (2013) *The Tallinn Manual on International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press, 215p.

Onuf, Nicholas. (1989) *World of Our Making: Rules and Rule in Social Theory and International Relations*. Columbia: University of South Carolina Press, 319p.

Portal Brasil. (2013). *Apresentado simulador nacional de guerra eletrônica* [http://www.brasil.gov. br/defesa-e-seguranca/2013/01/apresentado-simulador-nacional-de-guerra-eletronica]. Accessed 01/12/2015.

Portal Brasil. (2014). Amorim anuncia projeto de Escola de Defesa Cibernética. [http://www.brasil.gov. br/defesa-e-seguranca/2014/01/amorim-anuncia-projeto-de-escola-de-defesa-cibernetica]. Accessed 01/12/15.

Rohr, Altieres. (2014) NSA causou 'blecaute' na internet da Síria em 2012, diz Snowden. *Portal G1* [http://g1.globo.com/mundo/siria/noticia/2014/08/nsa-causou-blecaute-na-internet-da-siria-em-2012-diz-snowden.html]. Accessed 01/15/2015.

SYMANTEC. (2012) 2012 Norton cybercrime report. [http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf] Accessed 02/09/2015.

USA (2003). Department of Homeland Security*, The National Strategy to Secure Cyberspace*, (EUA). [https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf]. Accessed 01/15/2015.

USA. (2010) [PCNNA] Senate. Protecting Cyberspace as a National Asset Act (PCNNA), Bill S.3480, 2010. [http://thomas.loc.gov/cgi-bin/bdquery/z?d111:S3480:]. Accessed 01/14/2015.

USA. (1999) White House, *A National Security Strategy for a New Century* (EUA) [http://clinton4.nara.gov/media/pdf/nssr-1299.pdf]. Accessed 01/15/2015.

USA. White House, (2009) *Remarks by the President on Securing our Nation's Cyber Infrastructure* (EUA) [http://www.whitehouse.gov/the-press-office/remarks-president-securing-our-nations-cyber-infrastructure]. Accessed 01/16/15.

USA. White House, (2011) *International strategy for cyberspace: prosperity, security and openness in a networked world (EUA)* [http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf]. Accessed 01/15/2015.

Wæver, Ole. (2012). Aberystwyth, Paris, Copenhagen New 'Schools' in Security Theory and Their Origins between Core and Periphery. In *Thinking international relations differently*. Tickner, Arlene B.; Blaney, David L. eds. Nova York: Routledge, p.48-71.

Walt, Stephen M. (1991). The Renaissance of Security Studies. *International Studies Quarterly*, vol. 35, p. 211-239.

Acknowledgements

Luísa Cruz Lobato acknowledges the support from Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ). Kai Michael Kenkel acknowledges the support from Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPQ), Fundação Carlos Chagas Filho de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ), and Social Sciences Centre at

Pontifical Catholic University of Rio de Janeiro (CCS/PUC-Rio). Translation support was provided by Mariana Kalil.

Abstract

This paper uses the framework of the Copenhagen School to understand the process of securitization of cyberspace, exploring how something in such sphere becomes a threat. Seeking to contribute to the debate, this study analyses the securitization discourses of Brazil and of the United States from Hansen and Nissenbaum's (2009) theorization about the existence of a specific sector for cybersecurity. To comprehend the securitization of cyberspace in these terms allows not only to identify distinct levels of securitization, but also to capture the dynamics of cyber threats, distinguishing them from those existent in other sectors, as well as to trace distinctions between tendencies of securitization and militarization.

Keywords: Copenhagen School, Cyberspace, International Security, Securitization;.

Resumo

O presente artigo utiliza o quadro proposto pela Escola de Copenhagen para compreender a securitização do ciberespaço, explorando como algo nessa esfera se torna ameaça. Buscando-se contribuir no debate, analisa-se os discursos de securitização de Brasil e de Estados Unidos a partir da teorização de Hansen e Nissenbaum (2009) sobre a existência de um setor específico à segurança cibernética. Compreender a securitização do ciberespaço nesses termos, além de permitir identificar graus distintos de securitização, também permite capturar as dinâmicas das ameaças cibernéticas, distinguindo-as daquelas existentes em outros setores, bem como traçar distinções entre tendências de securitização e militarização.

Palavras-chave: Escola de Copenhagen; Ciberespaço; Segurança Internacional; Securitização.

Received: June 28, 2015
Accepted: October 13, 2015