A Discourse Analysis of Cyber Defense in Brazil

Oppermann, Daniel

Preprint / Preprint
Konferenzbeitrag / conference paper

7º Encontro da ABRI
Atores e Agendas: Interconexões, Desafios e Oportunidades

Belo Horizonte, PUC-Minas, 23 a 26 de julho de 2019
Área Temática: Segurança Internacional, Estudos Estratégicos e Política de Defesa

A DISCOURSE ANALYSIS OF CYBER DEFENSE IN BRAZIL

Daniel Oppermann
ECEME/FGV

Resumo:
Over the past ten years, cyber security and cyber defense have become widely discussed topics in Brazil. In the context of national defense, a careful discourse on cyber defense can be observed. The publication of the 2008 National Defense Strategy which includes references to the “cybernetic sector” has lead to a number of steps taken place mostly in the sphere of the Ministry of Defense to develop cyber defense strategies.

In parallel to such debates, an academic discourse is attending the procedures within the ministry. Part of this initial academic discourse resulted in a number of publications including a cyber defense guide developed by researchers from universities in Pernambuco, Santa Catarina, São Paulo and others.

The objective of this article is to analyze the contributions of the military and the academic sector regarding the debate on cyber defense in Brazil. To achieve this goal a discourse analysis will be conducted that uses methodological approaches originally developed by Michel Foucault and which were specified later by German researchers at the universities of Augsburg and Dortmund (Reiner Keller, Jürgen Link et al.) whose methodological works will be used as well. Another important source for the methodological design is the work of the constructivist copenhagen school, especially Lene Hansen and her discourse analysis methods on the war in Bosnia. The approaches of the researchers mentioned here were chosen to benefit from their relatively different directions regarding discourse analysis. While Foucault and the German researchers are extensively working with sociological approaches and literary studies, Hansen has adopted the same methodological approaches to the areas of International Relations and Security Studies. The experience drawn from her analysis will therefore be used as a central means to develop the final article on the discourse analysis of cyber defense in Brazil.

Palavras-chaves: defesa cibernética; análise de discurso; Brasil

Introduction

Academia is built upon history. It is such a short sentence that is able to sum up what researchers do when they think about academic theory development and academic research as a whole. For centuries, academics in all parts of the world depend on the understanding and interpretation of history to create and analyse knowledge. Deep going academic research always builds on knowledge, findings and theories that have been developed in the past. It is the state of the art in academic research to find out first about history and background information before developing new ideas and assumptions. Especially in the humanities and the social sciences researchers dig deep into theoretical developments of the past and use the outcomes to develop their own discourse.

The 20th century research and theory development of International Relations, Military and Security Studies, Political Science and others would not have been possible the way they came out if their early thinkers would not have borrowed from those that were discussing and noting down their thoughts on social environments centuries before. History is more than a number of dates, facts and occurrences. History is formed by the individuals writing it down. It is influenced by the assumptions and preferences of the writer, by theoretical knowledge and not to forget, by geographical location.

Academic research and theory building in Myanmar, Uganda or Chile (just to give some random examples) surely differs from that in Canada or France. It is history that often makes a difference when we think about social environments and experiences that help us form a theoretical approach. And nevertheless, large parts of academia in many regions of the world are ignoring their own environments or interests in favor of theoretical approaches or ideas that were developed under completely different circumstances.

In International Relations, Security and Military Studies academics borrow from concepts developed in Western Europe and North America during the Cold War when the principal or so-called classical ideas of these approaches were discussed and written down (inter alia: CARR, 2001; KEOHANE, 1986; MEARSHEIMER, 2014; MORGENTHAU et al, 2006; WALTZ, 1992). Cyber security, although not a concept of the Cold War but its aftermath, follows the same line. When nowadays students and academics all over the world study cyber security

and/or cyber defense they use for example historical experiences written down in North America since the 1950s when the first mainframe computers filled entire rooms and gave birth to what is now known as cybercrime (BRENNER, 2010; MCQUADE, 2006; WALL, 2011; YAR, 2013).

Historical approaches of cyber security research usually focus on what has happened in North America during the second half of the 20th century including the emergence of the first hacker groups at MIT, the first famous cases of professional cybercrime and cyber security incidents like the cookie monster, Kevin Poulsen's activities and more. The reason for people focussing on these or other examples is often quite simple. It is the absence of literature on their own (cyber) history, the lack of background data to understand where phenomena in different parts of the world are coming from. And while studying the interests of other countries is a completely common and recommended behaviour in academic research, the lack of literature and analysis regarding the own country and history is also what matters a lot.

Theoretical framework

Discussing theoretical approaches to security requires a first glance at the question how security is historically analyzed as a concept. Although issues of national and international security were already touched upon by so-called classical philosophers of the 15th and 16th century like Hobbes and Machiavelli, it was only in the 20th century that academics, driven by the experience of globally hot and cold wars, started conceptualizing security on a theoretical level to be able to develop a deeper understanding of the phenomenon itself.

An early and important contribution regarding the conceptualization of security was made by Buzan in 1983 in which he labeled security as an essentially contested concept, using the argument of Gallie (GALLIE, 1955). Following Gallie, it is necessary to differentiate between undisputed concepts and those that he called essentially contested, meaning concepts that are highly disputed and difficult to narrow down. Examples of essentially contested concepts given by Gallie are "democracy" and "art" which he analyzed in his work. While Schäfer (2013) and others agreed with Buzan there are also those questioning his conclusion. Baldwin for example discussed security under the Gallie argument but in the end of his analysis denied

“contestedness” in the sense of Gallie and instead attributes security to be “insufficiently explicated” (BALDWIN, 1997).

While theoretically conceptualizing security has taken and is still taking place in a selected number of moment, the academic conceptualization of cyber security is still in its early stages. At this moment, very few contributions to this debate are available and the number is getting even smaller when removing pure policy research approaches. While a suggested theoretical conceptualization of cyber security from the perspective of the European Union was published in 2018 (KOK, 2018) and also debates in North America around cyber security have improved over the years, researchers from CIS India have recently published a (policy) paper on conceptualizing a cyber security regime (BASU; HICKOK, 2018). At this moment, no substantial academic contribution regarding this question is known from Brazil (with the exception of policy documents which, however, hardly touch the question of conceptualization).

Regarding theoretical standpoints, cyber security can be debated using a number of approaches depending not only on the scope of the research project or the political orientation of the authors but also on the actual field of studies. Academics in the fields of Military Science and International Relations can choose from a number of approaches from classical realism over institutionalism to constructivism which today are considered to be among the principal approaches. Nevertheless, a growing number of sub-approaches has also made its way into academic debates on security, among them peace studies, critical security studies, human security studies, gender studies, securitization and more.

Cyberspace or cyber security, being relatively new topics of analysis, have so far often been discussed in the realms of state-centered realism with the scope of national cyber defense strategies, institutionalism in the context of international cooperation to tackle cyber attacks or cyber crime, and constructivism/securitization to analyze discourses on cyber security.

Methodology

Since the objective of this article is to analyze and discuss academic research on cyber security and cyber defense in Brazil and since research in this context must be understood as an

academic discourse set up by different individuals or organizations who are communicating directly or indirectly with one another, the method applied for this research process will be discourse analysis.

Discourse analysis, while being coined especially by Foucault since the 1970s, has different orientations and is used mainly in the social sciences but also in history and linguistic studies. The principal idea of discourse analysis is to categorize data like written documents, audio or video data of spoken words (or images) and to analyse them based on a set of variables like key expressions, theoretical ideas, arguments, objects, symbols, patterns etc with the objective to improve understanding of meaning and of possible impacts and consequences on a social environment. Andreas Heindl has identified three streams of discourse analysis being a normative-critical stream, an analytical-pragmatic stream and a genealogical-critical stream (HEINDL, 2015). In this context, he defines the normative-critical stream as an analysis of legitimacy in public debates and political discourse processes. This approach, which is also considered to be a discourse theory with less empirical impact, has gained acceptance for being a useful tool in understanding and shaping processes of political decision-making. The analytical-pragmatic approach however, is using empirical data analysis through quantitative and qualitative methods (ex: interviews, content analysis etc) to study not just language and communication but also the social context, the environment itself. And as a third line, Heindl mentions the genealogical-critical approach that was shaped especially by Foucault himself.

It is this third line that will be used for this research project since it is much more focused on the analysis of concepts, ideas and categorizations which are essential elements for an academic discourse (different than for example a discourse based on public speeches and political statements). Also, the extensive work of professor Reiner Keller of Augsburg University in Germany will be used to analyze the academic cyber defense discourse in Brazil (KELLER, 2011a, 2011b; KELLER et al., 2010, 2011; KELLER; HIRSELAND; SCHNEIDER, 2005; KELLER; SCHNEIDER; VIEHÖVER, 2012; KELLER; TRUSCHKAT, 2013; VIEHÖVER; KELLER; SCHNEIDER, 2013). Keller has published largely on discourse analysis methods for the past 15 years. Following his 2011a (p. 47) work on discourse research, the formation of objects (coming also from Foucault) can be delimited by specific questions including those of academic disciplines involved in the discourse. This questioning approach is of utter importance for this article which is in fact looking to define (besides other variables) the academic fields and

disciplines that are forming the Brazilian discourse on cyber security. Besides that, Keller mentions the importance of institutional spaces that are actively involved in a given discourse, being in this case individual universities or institutes in different parts of Brazil. The quantity and quality of contributions to a discourse are crucial elements to understand the importance of selected institutions (and individuals) to a given discourse. Under these circumstances, one could hypothetically argue that Brazilian researchers at Igarapé Institute have an equal or stronger voice in the Brazilian cyber security discourse than researchers at the Federal University of Rondônia, simply due to the fact that Igarapé is strategically located in Rio de Janeiro with access to larger media attention than researchers in Rondônia are, who however have published at least three times more on the same subject than Igarapé has.

For the study of international relations and security, a widely presented application of discourse analysis is rarely found in the literature. Lene Hansen's analysis of the Western discourse on the Bosnian war of the early 1990s is one of the few exceptions (HANSEN, 2006). Her methodological insights are therefore of a larger importance as well.

Cyber security and cyber defense in real world scenarios

In June 2011, a massive web defacement attack brought down a large number of government websites in Brazil, among them the website of the President, ministries, Petrobrás, the IBGE institute and several local state website from Acre to Rio Grande do Sul (OPPERMANN, 2014). It was the first large cyber attack that Brazil was officially confronted with but certainly not the first in the world. Since the commercial launch of the Internet in the early 1990s several countries, institutions and organizations in all parts of the world are frequently confronted with cyber attacks and organized malware intrusions. Although cyber attacks and criminal cyber activities have been around since the 1950s, long before the Internet or its predecessor, the ARPANET, started connecting networks in different countries, it was mostly the Estonia DDoS attacks in 2007 that managed to bring cyber security on the international agenda (MUELLER, 2013; OPPERMANN 2010).

Estonia, a pioneer network society in the Baltic region was suffering from the most aggressive act of cyber attacks that any nation state had experienced before. In the context of a local

conflict between Estonians and the Russian minority living in the country, concentrated DDoS attacks cut off all connections in the country bringing down public online life and economic transactions for a whole week. Estonia, being a financial hub in the region, lost millions of EUR transactions in those days causing damage to its own economy and its reputation as a reliable regional financial transaction center. The Estonian government and the whole European continent were taken by surprise. Although traditional investigations lead security analysts to the Russian territory they were unable to technically prove the origin of these cyber attacks.

As a consequence of the attacks, Estonia's capital Tallinn became home to the NATO Cooperative Cyber Defence Centre of Excellence shortly after, the first cyber security research and education center of the Western security alliance. Estonia was not the only case. Less than a year later, the Caucasian republic of Georgia was struck by cyber attacks during military conflicts over South-Ossetia with its neighbor Russia. On that occasion, Russian traditional military attacks were facilitated by coordinated timely cyber attacks on Georgian infrastructure.

While both of these cases were openly visible aggressions against sovereign countries, other well known examples of subliminal cyber attacks also exist. The most discussed over the past years was the case of Stuxnet, a worm infiltrating and damaging specific industrial infrastructure of the German company Siemens in the year 2010, that was used to run nuclear installations in Iran (CLARKE; KNAKE, 2012; LOPES; JOST DE OLIVEIRA, 2014; VALERIANO; MANESS, 2015). Differently than the cases of Estonia and Georgia, the Stuxnet activities were not visible to the public. It even was not clear to the Iranian authorities who were only able to identify frequently inoperable parts in a number of nuclear power plants. European IT specialists managed to discover the Stuxnet worm shortly after it accidentally escaped from Iranian infrastructure and made its way through the Internet. Technical analysts suggested the U.S. government being responsible for the development of the Stuxnet worm to cause damage to the Iranian nuclear energy program which at that time was a matter of international dispute. Two years later, the U.S. government admitted being responsible for the development of the worm which was a cooperation project with the state of Israel.

Compared to Estonia, Georgia and Iran, Brazil's web defacement attacks in 2011 were a case of minor severity which caused little international attention. Nevertheless, it brought a problem to the public and the political agenda that had not received too much attention in the years before:

the vulnerability of public and crucial infrastructure in the times of global networks and mostly uncontrolled data flow. A few months before the web defacement attacks took place, which were conducted by different anonymous hacker groups without a precisely defined political agenda, Brazil had already taken a first important step to put cyber security on its national agenda. This was the launch of the Green Book on Cyber Security published by the Department of Information and Communication Security (Departamento de Segurança da Informação e Comunicações, DSIC) within the Office of Institutional Security (Gabinete de Segurança Institucional da Presidência da República, GSI/PR) (MANDARINO JR.; CANONGIA, 2010). This document, although not further developed in the following years, marked an important moment to bring cyber security to the country's public agenda. It might be considered a follow-up of the 2008 National Defense Strategy published by the Ministry of Defense in which cyberspace was mentioned several times to be a future factor of national security. Although this strategy paper did not elaborate further on the issue it made clear that cyber security had entered the national security agenda.

What followed was a slight increase of debates (and further outputs) on cyber security and cyber defense on the governmental level which was also reflected in the organization of the CDCiber Center within the Ministry of Defense in 2010. CDCiber, also known as the Cyber Defense Center, has since then operated in a number of occasions like international sports events taking place in the country over the years (ABDENUR 2014). Since 2014, a National School of Cyber Defense is in preparation.

Cyber security and cyber defense in academia

While cyber security and cyber defense as public policy issues are slowly receiving more importance there is still a lack of academic debates on the topics in the national universities. Before the web defacement attacks, little had been published in Brazil from an academic perspective, but over the years the number of publications has been growing. While media outlets and Internet security companies are addressing the topic for many years, universities (especially in the fields of International Relations, Political Science etc) seem to be reluctant so far in giving stronger focus on cyber security research from an academic perspective. Academic publications on cyber security coming from Brazil are quite often developed by academics who

might have touched on a number of topics over the years or worked on international security issues in general but who are not specialized in IT or cyber security issues (yet). In fact, cyber security is a multidisciplinary area of studies that includes not just Political Science, International Relations and Security or Military Studies but which also requires technical knowledge from the areas of computing, programming or IT engineering.

Besides the dilemma of having relatively little academic research on cyber security and cyber defense in Brazil, many “prominent” publications and researchers are concentrated in the urban centers of the South-East of the country. While this is understandable on the one hand since urban centers in the states of Rio de Janeiro, Minas Gerais and São Paulo offer a high concentration of technology and Internet services in the country and as a consequence also the highest number of individuals observing and analyzing these scenarios, it also shows, on the other hand, an unequal representation of academics from other parts of the country. Regionally concentrating academic and policy debates means missing valuable contributions developed by academics in other parts of the country. And in fact, there are contributions from researchers in Santa Catarina like Danielle Ayres (UFSC) and Gills Lopes from Rondônia (UNIR) just as academics from Rio de Janeiro like Adriana Abdenur (Instituto Igarapé) or Samuel César da Cruz Júnior from IPEA, Brasília. But not only researchers from International Relations (as most of those mentioned before) are contributing to the debates on cyber security and/or defense. Also academics from other social sciences, engineering, informatics and law are developing ideas within the national debates in Brazil.

Conclusion

The academic debate on cyber security and cyber defense in Brazil is not following any predefined structure or conceptual approach. As mentioned above, the number of academics working continuously (and for a longer time) on cyber security, especially from an International Relations background (or similar) is relatively small, but growing. When we look at the continuity of these works we can find out that it is still rare (one exception is Lopes, writing on the topic since at least 2011). Only recently new researchers can be found having touched on the topic as well. Among them are Danielle Ayres (UFSC), Thiago Borne Ferreira (UFRGS), Flávio Rocha de Oliveira (UFABC), Cauê Rodrigues Pimentel (USP), Adriano Mauro Cansian (UNESP), Tatiana

Teixeira (UERJ) and Carlos André de Melo Alves (UnB). It is not clear though at this moment, if the before mentioned are actively pursuing a continued research agenda on cyber security. One exception here is Ayres who is publishing on cyber defense on a frequent basis for at least two years now.

Over the years, several researchers in Brazil touched cyber security as part of a general security research agenda. Mentioned here is Adriana Abdenur, researcher at the Igarapé Institute, who in 2014 discussed national cyber security in the context of the Snowden revelations for the Adenauer Foundation in Rio de Janeiro (ABDENUR, 2014). In her contribution, Abdenur draws a chronological line from the 2008 National Security Strategy over the 2010 Greenbook on Cyber Security until the foundation of the CDCiber Center in 2012. She presents CDCiber as an operational center for back then upcoming international sports events like the Olympic Games and the FIFA World Cup. Furthermore, she stresses the regional cooperation on cyber security education between Brazil and Argentina.

Besides Abdenur, also professor Gills Lopes of the Federal University of Rondônia develops his work on cyber security focussing on regional integration and in this context, following an institutionalist approach, the function of the Organization of American States (LOPES; MEDEIROS, 2011). Lopes has picked up and discussed a concept called CyberIR meaning Cyber International Relations (LOPES; MEDEIROS, 2018). In this concept he includes cyber security approaches plus other topics bringing together International Relations and cyberspace. CyberIR is a concept that has recently been used by MIT researchers in cooperation with the US Department of Defense to reflect on 21st century cyber challenges for the study of International Relations (CHOUCRI, 2015). Others have used the same term before to define cyber information retrieval, a technical approach to fight cybercrime (CHOU; CHANG, 2008). Lopes also uses, different than above, classical realist approaches to discuss cyber warfare. In his 2017 article for Carta Internacional he discusses, together with Freitas and Teixeira, aspects of traditional warfare in cyberspace (LOPES; FREITAS; TEIXEIRA, 2017).

Another publication from Brazil touching issues of cybersecurity is a 2014 special edition of the Adenauer Foundation's Cadernos Adenauer titled Cibersegurança, a collection of five articles touching on different dimensions of cybersecurity (DANE, 2014). For researchers of International Relations and International Security the contributions of Muggah/Glenn/Diniz regarding

securitization of cyberspace in Brazil might be of interest just as Dornsbusch's take on military operations in cyberspace. The remaining three chapters are approaching cyber security from a legal, sociological and RI point of view while not necessarily touching on aspects of international security but on information security and user data protection, national Internet and data legislation and soft power on the Internet. What is missed out in the publication is a conceptual debate about what cyber security actually means. Instead, the readers get confronted with a variety of different topics that are not set into a structural thematic framework.

Also following a constructivist approach is the 2015 contribution of Lobato and Kenkel on cyberspace securitization (LOBATO; KENKEL, 2015). Following the theoretical approach of the Copenhagen School the article aims at comparing cyber security discourses in the USA and Brazil. Very little content of the article, however, is actually touching on Brazil or a possible discourse of the topic in the country. The largest part of the article discusses the transatlantic discourse on cyber security (North-America and Europe).

The findings presented above are a first step to analyze cyber defense and cyber security debates in Brazil. Since the underlying research project is ongoing, more comprehensive results will be presented in the coming months.

Bibliography

ABDENUR, A. Brazil and Cybersecurity in the Aftermath of the Snowden Revelations. Multilateral Security Governance, XI. Forte de Copacabana, p. 229–242, 2014.

BALDWIN, D. A. The concept of security. Review of International Studies, v. 23, n. 1, p. 5–26, jan. 1997.

BASU, A.; HICKOK, E. Conceptualizing an International Security Regime for Cyberspace, Global Commission on the Stability of Cyberspace, The Hague Centre for Strategic Studies, 2018.

BRENNER, S. W. Cybercrime: criminal threats from cyberspace. Santa Barbara, Calif: Praeger, 2010.

BUZAN, B. People, states, and fear: the national security problem in international relations. Brighton: Wheatsheaf Books, 1983.

CARR, E. H.; COX, M. The twenty years' crisis, 1919-1939: an introduction to the study of international relations. reissued with a new introduction and additional material ed. Basingstoke, Hampshire: Palgrave, 2001.

CHOU, S.; CHANG, W. CyberIR – A Technological Approach to Fight Cybercrime. (C. C. Yang et al., Eds.) Intelligence and Security Informatics. Anais. Springer Berlin Heidelberg, 2008

CHOUCRI, N. Explorations in Cyber International Relations: A Research Collaboration of MIT and Harvard University, Research Paper No. 2016-1, Political Science Department, Massachusetts Institute of Technology, 2015.

CLARKE, R. A.; KNAKE, R. K. Cyber war: the next threat to national security and what to do about it. 1st Ecco pbk. ed ed. New York: Ecco, 2012.

DANE, F. (ED.). Cibersegurança. Rio de Janeiro: Konrad Adenauer Stiftung, 2014.

DINIZ, G.; MUGGAH, R.; GLENNY, M. Deconstructing cyber security in Brazil, Strategic Paper 11, Instituto Igarapé, 2014.

DSOUZA, Z. Are Cyber Security Incident Response Teams (CSIRTs) Redundant or Can They Be Relevant to International Cyber Security? Federal Communication Law Journal, v. 69, n. 3, p. 201–226, 2018.

FOUCAULT, M. The archaeology of knowledge. New York, NY: Pantheon Books, 1982.

FOUCAULT, M. et al. The hermeneutics of the subject: lectures at the Collège de France, 1981-1982. 1st ed ed. New York: Palgrave-Macmillan, 2005.

FOUCAULT, M.; KHALFA, J. History of madness. New York: Routledge, 2006.

GALLIE, W. B. Essentially Contested Concepts. Proceedings of the Aristotelian Society, v. 56, p. 167–198, 1955.

HABERMAS, J. Theorie des kommunikativen Handelns. 10. Aufl ed. Frankfurt/Main: Suhrkamp, 2016.

HANSEN, L. Security as Practice: Discourse analysis and the Bosnian war. London: Routledge, 2006.

HEINDL, A. Diskursanalyse. In: HILDEBRANDT, A. et al. (Eds.). Methodologie, Methoden, Forschungsdesign. Wiesbaden: Springer VS, 2015. p. 257–298.

HUREL, L. M.; CRUZ LOBATO, L. Uma Estratégia para a Governança da Segurança Cibernética no Brasil, Instituto Igarapé, Rio de Janeiro, 2018.

KELLER, R. et al. (EDS.). Handbuch Sozialwissenschaftliche Diskursanalyse. Band 2: Forschungspraxis. 4. Auflage ed. Wiesbaden: VS Verlag, 2010.

KELLER, R. Diskursforschung: eine Einführung für SozialwissenschaftlerInnen. 4. Auflage ed. Wiesbaden: VS Verlag, 2011a.

KELLER, R. et al. (EDS.). Handbuch sozialwissenschaftliche Diskursanalyse. Band 1: Theorien und Methoden. 3., erweiterte Auflage ed. Wiesbaden: VS Verlag, 2011.

KELLER, R. Wissenssoziologische Diskursanalyse: Grundlegung eines Forschungsprogramms. 3. Aufl ed. Wiesbaden: VS, Verl. für Sozialwiss, 2011b.

KELLER, R.; HIRSELAND, A.; SCHNEIDER, W. (EDS.). Die diskursive Konstruktion von Wirklichkeit. Köln: Halem, 2005.

KELLER, R.; SCHNEIDER, W.; VIEHÖVER, W. (EDS.). Diskurs - Macht - Subjekt: Theorie und Empirie von Subjektivierung in der Diskursforschung. 1. Aufl ed. Wiesbaden: VS, Verl. für Sozialwiss, 2012.

KELLER, R.; TRUSCHKAT, I. (EDS.). Methodologie und Praxis der Wissenssoziologischen Diskursanalyse. Bd. 1: Interdisziplinäre Perspektiven. Wiesbaden: Springer VS, 2013.

KEOHANE, R. O. (ED.). Neorealism and its critics. New York: Columbia Univ. Pr, 1986.

KOK, A. Conceptualizing Cyber-Security From EU Perspective. Proliferation of Open Government Initiatives and Systems, p. 143–154, 2018.

LOBATO, L. C.; KENKEL, K. M. Discourses of cyberspace securitization in Brazil and in the United States. Revista Brasileira de Política Internacional, v. 58, n. 2, p. 23–43, dez. 2015.

LOPES, Gills. Análise Exploratória da Securitizacão Militar do Ciberespaço nos EUA, Brasil e Canadá. SECURITY AND DEFENSE STUDIES REVIEW, v. 15, p. 116-138, 2014.

LOPES, G. Vigilância Cibernética no Brasil: O Caso Snowden sob o PRISMa de um insider. Revista Eco-Pós (Online), v. 18, p. 261-265, 2015.

LOPES, G.; FREITAS, M. T. D.; TEIXEIRA JR, W. M. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. Carta Internacional, v. 12, p. 30-53, 2017.

LOPES, G.; JOST DE OLIVEIRA, C. F. Stuxnet e defesa cibernética estadunidense à luz da análise de política externa. Revista Brasileira de Estudos de Defesa, v. 1, n. 1, p. 55–69, 2014.

LOPES, G.; MEDEIROS, M. A. . CiberRI ou introdução aos estudos sistemáticos sobre o ciberespaço no tripé ensino-pesquisa-extensão de Relações Internacionais. MERIDIANO 47 (UNB), v. 19, p. 1-20, 2018.

LOPES, G.; MEDEIROS, M. A. . Da cibersegurança à ciberdefesa Americana: a diplomacia da internet como instrumento de proteção e de integração dos estados da OEA. In: 3º Encontro Nacional ABRI, 2011, São Paulo. Anais do 3° ENABRI 2011 3° Encontro Nacional ABRI 2011. São Paulo: USP, 2011.

MCQUADE, S. C. Understanding and managing cybercrime. Boston: Pearson/Allyn and Bacon, 2006.

MEARSHEIMER, J. J. The tragedy of great power politics. Updated edition ed. New York London: W.W. Norton & Company, 2014.

MORGENTHAU, H. J.; THOMPSON, K. W.; CLINTON, W. D. Politics among nations: the struggle for power and peace. 7. ed ed. Boston: McGraw-Hill Higher Education, 2006.

MUELLER, M. L. Networks and States: The Global Politics of Internet Governance. Reprint edition ed. Cambridge, Mass.: The MIT Press, 2013.

OPPERMANN, D. A necessidade de investigar a segurança cibernética no Brasil. Boletim OPSA, n. 6, p. 17, 2009.

OPPERMANN, D. Virtual attacks and the problem of responsibility: the case of China and Russia. Carta Internacional, v. 5, n. 2, p. 11–25, 2010.

OPPERMANN, D. Entre hackers e botnets: a segurança cibernética no Brasil. Boletim OPSA, n. 02, p. 12–16, 2011.

OPPERMANN, D. Internet Governance and Cyber Security in Brazil. Multilateral Security Governance, XI. Forte de Copacabana. p. 167–181, 2014a.

OPPERMANN, D. O cenário de cibersegurança depois de Snowden e consequências no Brasil. In: DUARTE, R. (Ed.). . Metamorfoses da violência (1914-2014). Janus Anuário de Relações Exteriores. Lisboa: Observare, Universidade Autónoma de Lisboa, 2014b. p. 148–149.

OPPERMANN, D. Governança da Internet e Segurança Cibernética no Brasil. Monções: Revista de Relações Internacionais da UFGD, v. 2, n. 4, p. 259–283, 2013.

SCHÄFER, P. J. Human and Water Security in Israel and Jordan. Heidelberg ; New York: Springer, 2013.

STAHL, B.; WALL, J.; DAYNES, S. Critical Discourse Analysis as a Theory and Review Methodology. In: TWENTIETH AMERICAS CONFERENCE ON INFORMATION SYSTEMS. Savannah: 2014.

VALERIANO, B.; MANESS, R. C. Cyber war versus cyber realities: cyber conflict in the international system. Oxford ; New York: Oxford University Press, 2015.

VIEHÖVER, W.; KELLER, R.; SCHNEIDER, W. (EDS.). Diskurs - Sprache - Wissen: interdisziplinäre Beiträge zum Verhältnis von Sprache und Wissen in der Diskursforschung. Wiesbaden: Springer VS, 2013.

WALL, D. S. Cybercrime: the transformation of crime in the information age. Cambridge: Polity Press, 2011.

WALTZ, K. N. Man, the state and war: a theoretical analysis. New York: Columbia Univ. Press, 1992.

YAR, M. Cybercrime and society. 2nd ed ed. Los Angeles: SAGE, 2013.